

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

17.06.99

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1998年10月29日

出 願 番 号
Application Number:

平成10年特許願第309223号

出 願 人
Applicant(s):

三菱マテリアル株式会社

REC'D 02 JUL 1999

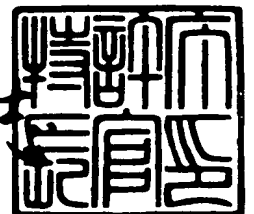
WIPO PCT

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

1999年 4月 9日

特 許 庁 長 官
Commissioner,
Patent Office

伴佐山 建志



出証番号 出証特平11-3021093

【書類名】 特許願

【整理番号】 J75130A1

【提出日】 平成10年10月29日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 11/00

【発明の名称】 チームデータリスト管理装置及びチームデータリスト保管装置及びチームデータリスト処理システム、並びに、それらの記録媒体

【請求項の数】 8

【発明者】

【住所又は居所】 埼玉県大宮市北袋町1丁目297番地 三菱マテリアル株式会社 総合研究所内

【氏名】 大久保 達真

【発明者】

【住所又は居所】 埼玉県大宮市北袋町1丁目297番地 三菱マテリアル株式会社 総合研究所内

【氏名】 中根 一成

【特許出願人】

【識別番号】 000006264

【氏名又は名称】 三菱マテリアル株式会社

【代理人】

【識別番号】 100064908

【弁理士】

【氏名又は名称】 志賀 正武

【選任した代理人】

【識別番号】 100108578

【弁理士】

【氏名又は名称】 高橋 詔男

【選任した代理人】

【識別番号】 100089037

【弁理士】

【氏名又は名称】 渡邊 隆

【選任した代理人】

【識別番号】 100101465

【弁理士】

【氏名又は名称】 青山 正和

【選任した代理人】

【識別番号】 100094400

【弁理士】

【氏名又は名称】 鈴木 三義

【選任した代理人】

【識別番号】 100106493

【弁理士】

【氏名又は名称】 松富 豊

【選任した代理人】

【識別番号】 100107836

【弁理士】

【氏名又は名称】 西 和哉

【選任した代理人】

【識別番号】 100108394

【弁理士】

【氏名又は名称】 今村 健一

【選任した代理人】

【識別番号】 100108453

【弁理士】

【氏名又は名称】 村山 靖彦

【選任した代理人】

【識別番号】 100100077

【弁理士】

【氏名又は名称】 大場 充

【手数料の表示】

【予納台帳番号】 008707

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704954

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 チームデータリスト管理装置及びチームデータリスト保管装置
及びチームデータリスト処理システム、並びに、それらの記録媒体

【特許請求の範囲】

【請求項1】 チームを階層化するためのチームデータリストを管理するチームデータリスト管理装置であって、

所定の要求先に前記チームデータリストの操作要求を行い、該操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名を含むオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名を含むオーソリティリストを有するチームデータリストを前記要求先から取得し、前記識別子を用いて取得されたチームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストの電子署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者による署名であることを確認して、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認手段と、

該正当性確認手段によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加えるチームデータリスト変更手段と、

前記操作要求を行った指示者の電子署名を作成し、前記変更されたチームデータリストに該電子署名を添付して前記要求先に送出する署名手段と

を具備することを特徴とするチームデータリスト管理装置。

【請求項2】 前記管理者情報は、前記チームマスタにより自チーム内のメンバーから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報であることを特徴とする請求項1記載のチームデータリスト管理装置。

【請求項3】 前記ルートチームのチームマスタの本人識別を行うための識別情報を所定の場所から取得して登録する登録手段と、

予め登録されている前記識別情報を用いて、前記要求先から送られてくる前記

ルートチームのオーソリティデータの電子署名が前記チームマスタの電子署名であることを確認するチームマスタ確認手段とをさらに有することを特徴とする請求項 1 又は 2 記載のチームデータリスト管理装置。

【請求項 4】 チームを階層化するためのチームデータリストを保管するチームデータリスト保管装置であって、

自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータをチーム毎に記憶するオーソリティデータ記憶手段と、

自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストをチーム毎に記憶するオーソリティリスト記憶手段と、

前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する所定の要求元からの操作要求について、該操作要求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、参照要求或いは削除要求に対して要求されたチームデータリストを前記要求元へ返送し或いは削除し、更新要求に対しては、前記要求元から送られるチームデータリストの電子署名が権限を持つ者による署名であることを前記管理者情報を用いて確認し、前記送られたチームデータリストで前記オーソリティデータ記憶手段及び前記オーソリティリスト記憶手段の記憶内容を更新する権限確認手段と

を具備することを特徴とするチームデータリスト保管装置。

【請求項 5】 前記管理者情報は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報であることを特徴とする請求項 4 記載のチームデータリスト保管装置。

【請求項 6】 要求元である請求項 1～3 の何れかの項記載のチームデータリスト管理装置と、

要求先である請求項 4 又は 5 記載のチームデータリスト保管装置とを有することを特徴とするチームデータリスト処理システム。

【請求項 7】 チームを階層化するためのチームデータリストを管理するチ

ームデータリスト管理プログラムを記録した記録媒体であって、

所定の要求先に前記チームデータリストの操作要求を行う処理と、

前記操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストを有するチームデータリストを前記要求先から取得する処理と、

前記識別子を用いて取得された各チームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストの電子署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者による署名であることを確認したのち、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認処理と、

該正当性確認処理によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加える変更処理と、

前記操作要求を行った指示者の電子署名を作成して、前記変更処理によって変更されたチームデータリストに該電子署名を添付して前記要求先に送出する処理と

をコンピュータに実行させるためのチームデータリスト管理プログラムを記録した記録媒体。

【請求項8】 チームを階層化するためのチームデータリストを保管するチームデータリスト保管プログラムを記録した記録媒体であって、

自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータをチーム毎に予め記憶しておく処理と、

自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストをチーム毎に予め記憶しておく処理と、

所定の要求元から前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する操作要求があったときに、該操作要

求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、該操作要求が参照要求或いは削除要求である場合は、要求されたチームデータリストを前記要求元へ返送し或いは削除し、該操作要求が更新要求である場合は、前記要求元から送られるチームデータリストの電子署名が権限を持つ者による署名であることを前記管理者情報を用いて確認したのち、前記送られたチームデータリストで記憶されている前記オーソリティデータ及び記憶されている前記オーソリティリストを更新する権限確認処理と

をコンピュータに実行させるためのチームデータリスト保管プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、複数のユーザ（メンバ）から構成される企業の部や課といったチームを階層化するためのチームデータリストを作成、管理、保管してゆくとともに、ユーザに提供される各種の情報や様々な機能をユーザ間で安全に共有するためのチームデータリスト処理システムに関するものである。さらに詳細には、チームデータリストの保管に係わる処理を担うチームデータリスト保管装置と、チームデータリスト保管装置上から取得したチームデータリストを対象に様々な管理を行うチームデータリスト管理装置を備えたシステムに関するものである。

【0002】

【従来技術】

ユーザに提供される各種の機能や情報といった様々な資源を複数のユーザ間で共有するためには、これら資源にアクセスを要求しているユーザが、本当に資源へアクセスする権利を有しているのか否かを検証する機能を用意しておく必要がある。かかる検証を行うために、従来は、資源に対する正当なアクセス権限を付与されたユーザを予め定義したアクセスコントロールリスト（以下、「ACL」と略記する）と呼ばれるリストを利用している。なお、ここで言うACLは、上述したチームデータリストに含まれる種々の情報のうち、共有資源に対するアクセスを制御するための情報だけが含まれたリストの一例である。

【0003】

図15は、ACLを利用して複数のユーザ間で情報共有を行う従来のシステムの概要を示したものである。同図に示されるシステムでは、イントラネット1、インターネット2がそれぞれファイアウォール3、4を介してサーバ5に接続されており、イントラネット1内部の者ばかりでなく、イントラネット外の共有メンバー6がインターネット2を介して互いに情報を共有している。周知のように、イントラネット1は企業内に整備されたネットワークなどの閉じたネットワークであり、その一方で、インターネット2は世界中にまたがるパブリックなネットワークである。

【0004】

また、ファイアウォール3、4は悪意を持った侵入者などがイントラネット1へ不正にアクセスすることを防止するためのコンピュータである。サーバ5は各種の資源が蓄積されている端末（コンピュータ）であって、共有情報が格納されたデータベース7と、特定の情報ないし機能にアクセスしても良いグループ及びそれに属するメンバーのメンバーリストを保持したACL8を備えている。このサーバ5は、データベース7に蓄積されている共有情報を管理するデータ保管機能のほか、クライアントに相当する通信相手が予め許可されている者か否かを検証するユーザ認証機能、ACL8に基づいて共有情報に対するアクセスの可否を検証するアクセス制御機能、ACL8に基づいて特定のグループに属するメンバーだけが特定の共有情報へアクセスすることを可能ならしめるグループ管理機能を備えている。

【0005】

図15のシステムでは、共有メンバー6やイントラネット1内部のユーザからデータベース7に対するアクセス要求があると、サーバ5はその都度ACL8を参照してユーザ認証を行い、当該ユーザがメンバーとしてACL8に定義されていればアクセスを許可し、メンバーとして定義されていなければアクセスを拒否する。また、当該ユーザに対してアクセスが許可されている場合、サーバ5はACL8を参照して当該メンバーが特定のグループに含まれるかどうかを確認するとともに、当該メンバーがアクセス要求のある共有情報に関してアクセスを許されているか

どうか調べるようにしている。

【0006】

【発明が解決しようとする課題】

ところで、複数のユーザ間で資源を共有する場合にはサーバ側の管理者を共有メンバに含めるのが好ましくない場合もある。例えば、ある企業の情報システム部に所属するシステム管理者は、人事部内だけで共有すべき企業の人事情報にアクセス不可能であることが必要と考えられる。ところが、上述した図15のようなシステムでは、サーバ5の管理者に対してACL8の設定や管理を行う権限を許与してしまっている。そのため、サーバ管理者5がACL8に対して不正なアクセスを行うことが可能であり、意図的にACL8の設定内容が改竄されるのを防止することができない欠点がある。これに加えて、サーバ管理者以外にも、サーバSVへ不正に侵入する者（いわゆるクラッカ）によってACL8が不正に改竄されてしまうおそれもある。

【0007】

このほか、企業内部で情報を共有してゆく利用形態などへの適用を考えた場合、そうした形態にうまく適合したシステムを構築してゆくことが望ましい。すなわち、ある程度以上の規模の企業では組織がピラミッド状に形成された階層関係になっており、例えば、人事部の配下には人事一課や人事二課が設置されていることなどはごく一般的であると言える。また、開発部門などでは商品の開発工程などに合わせて例えば開発部長が新たに課を作ったり、幾つかの課を統合したり、あるいは、ある特定の課を廃止したりする権限が与えられている場合も考えられる。また、それぞれの課が業務別にいくつかのグループに分かれていることもある。

【0008】

そうした組織にあっては、開発部長が各課やそれぞれの課に属する全てのグループの構成員を管理することは非常な負担である。そこで、こうした管理負担を分散するために、開発部長を補佐する者を何人か割り当てるようにしてこれらの者に管理業務の一部又は全部を代行させることなどが行われている。さらには、開発部長には課の作成、統廃合等の業務を行う権限だけを与えておき、課内部の

管理や情報共有自体は課長やその下のグループリード等に一任するといった形態が採られている。しかるに、上述した従来のシステムではいま説明したような企業の組織形態に適合した柔軟な管理や情報共有は何ら考慮されていないという問題がある。

【0009】

本発明は上記の点に鑑みてなされたものであり、その目的は、サーバの管理者といった特権者も含め、企業の組織単位等に相当するチームの外にいる者、クラッカ等がチームデータリストに不正を行うことを防止しつつ、チームの階層化および各種の情報や機能の実現するためのチームデータリスト処理システムを提供することにある。さらに詳しくは、各チームに所属しているメンバから特に選ばれた者だけが、チームの配下にサブチームを作成したり、サブチームの作成権限を特定の複数人に割り当てたり、サブチームの作成権限者が選定した特定人にサブチーム内の管理を行わせたりすることが可能なチームデータリスト処理システムを提供することにある。

【0010】

【課題を解決するための手段】

以上の課題を解決するために、請求項1記載の発明は、チームを階層化するためのチームデータリストを管理するチームデータリスト管理装置であって、所定の要求先に前記チームデータリストの操作要求を行い、該操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名を含むオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名を含むオーソリティリストを有するチームデータリストを前記要求先から取得し、前記識別子を用いて取得されたチームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストの電子署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者による署名であることを確認して、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認手段と、該正当性確認手段によって正当性が確認された前記チームデータリストに対して前記操作要

求に応じた変更を加えるチームデータリスト変更手段と、前記操作要求を行った指示者の電子署名を作成し、前記変更されたチームデータリストに該電子署名を添付して前記要求先に送出する署名手段とを具備することを特徴としている。

【0011】

また、請求項2記載の発明は、請求項1記載の発明において、前記管理者情報は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報であることを特徴としている。

また、請求項3記載の発明は、請求項1又は2記載の発明において、前記ルートチームのチームマスタの本人識別を行うための識別情報を所定の場所から取得して登録する登録手段と、予め登録されている前記識別情報を用いて、前記要求先から送られてくる前記ルートチームのオーソリティデータの電子署名が前記チームマスタの電子署名であることを確認するチームマスタ確認手段とをさらに有することを特徴としている。

【0012】

また、請求項4記載の発明は、チームを階層化するためのチームデータリストを保管するチームデータリスト保管装置であって、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータをチーム毎に記憶するオーソリティデータ記憶手段と、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストをチーム毎に記憶するオーソリティリスト記憶手段と、前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する所定の要求元からの操作要求について、該操作要求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、参照要求或いは削除要求に対して要求されたチームデータリストを前記要求元へ返送し或いは削除し、更新要求に対しては、前記要求元から送られるチームデータリストの電子署名が権限を持つ者による署名であることを前記管理者情報を用いて確認し、前記送られたチームデータリ

ストで前記オーソリティデータ記憶手段及び前記オーソリティリスト記憶手段の記憶内容を更新する権限確認手段とを具備することを特徴としている。

また、請求項5記載の発明は、請求項4記載の発明において、前記管理者情報は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報であることを特徴としている。

また、請求項6記載の発明は、要求元である請求項1～3の何れかの項記載のチームデータリスト管理装置と、要求先である請求項4又は5記載のチームデータリスト保管装置とを有することを特徴としている。

【0013】

また、請求項7記載の発明は、チームを階層化するためのチームデータリストを管理するチームデータリスト管理プログラムを記録した記録媒体であって、所定の要求先に前記チームデータリストの操作要求を行う処理と、前記操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストを有するチームデータリストを前記要求先から取得する処理と、前記識別子を用いて取得された各チームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストの電子署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者による署名であることを確認したのち、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認処理と、該正当性確認処理によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加える変更処理と、前記操作要求を行った指示者の電子署名を作成して、前記変更処理によって変更されたチームデータリストに該電子署名を添付して前記要求先に送出する処理とをコンピュータに実行させることを特徴としている。

【0014】

また、請求項8記載の発明は、チームを階層化するためのチームデータリストを保管するチームデータリスト保管プログラムを記録した記録媒体であって、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータをチーム毎に予め記憶しておく処理と、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストをチーム毎に予め記憶しておく処理と、所定の要求元から前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する操作要求があったときに、該操作要求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、該操作要求が参照要求或いは削除要求である場合は、要求されたチームデータリストを前記要求元へ返送し或いは削除し、該操作要求が更新要求である場合は、前記要求元から送られるチームデータリストの電子署名が権限を持つ者による署名であることを前記管理者情報を用いて確認したのち、前記送られたチームデータリストで記憶されている前記オーソリティデータ及び記憶されている前記オーソリティリストを更新する権限確認処理とをコンピュータに実行させることを特徴としている。

【0015】

【発明の実施の形態】

以下、図面を参照して本発明の実施形態について説明するが、まず初めに本発明におけるチームデータリストについて説明する。本発明におけるチームデータリストは、チームに関する情報を定義したリストの総称であって、上述したACLのような機密性の高い管理が要求される用途に適用される「メンバーの集合」を定義するためのものである。上述した通り、従来のシステムでは、チームのメンバーではない端末管理者、ネットワーク管理者、サーバ管理者などがチームに関する情報を変更することができる。一方、本発明におけるチームデータリストでは、チームに関する情報を複数のリスト（後述するようなオーソリティリスト、オーソリティデータやメンバーリスト、チームマスタリスト、アプリケーションリスト）に分割して管理することで、チームの階層化やチームマスタ自身の変更といったチーム管理をチーム内のメンバーだけで行えるようにしている。

【0016】

以下に詳述する実施形態では、第一に、チームの配下にサブチームを作成できるようにして、会社組織等における階層関係を模擬して情報共有を行ってゆく仕組みを実現している。第二には、特に選定された複数の人間に対してサブチームの作成権限を授与できるような仕組みを実現しており、それによって一人の管理者に負荷が集中しないようにして管理負担の分散を図っている。第三には、サブチーム内部の管理については、サブチーム作成権限者がサブチーム内から選んだ特定の者に行わせる仕組みを実現している。そうすることによって、チームの管理者がサブチーム内部の管理や情報共有に関与しなくとも済むようにしている。

【0017】

〔第1実施形態〕

本実施形態では、階層化されたチームに合わせて、チームデータリストにアクセスできる者をその権限の内容に応じてメンバ、サブオーソリティ、チームマスタの3種類に分類しており、この順番でその者に付与される権限が拡大してゆく。チームマスタは或るチームの管理者であって、当該チームの配下の組織たるサブチームの作成といった管理権限を有する者である。一方、サブオーソリティはチームマスタによって指名された者であって、チームマスタと同様にサブチームの作成といった管理権限を持つ者であるが、他の者をサブオーソリティとして指名することは許されていない。サブオーソリティは複数人いる場合もあれば一人もいない場合もある。他方、サブオーソリティ及びチームマスタ以外の一般のメンバは情報や機能を共有する者であって、サブチームの作成権限などの特権はいっさい与えられていない。なお、サブオーソリティやチームマスタは特別な権限が与えられてはいるが、チーム内のメンバであることに変わりはなく、その意味でサブオーソリティやチームマスタをメンバと呼ぶこともある。なお、以下の説明及び図面ではチームマスタを「TM」と略記し、サブオーソリティを「sub AU」と略記することがある。

【0018】

以下、チームデータリスト管理装置及びチームデータリスト保管装置の2つの装置を備えたシステムについて本実施形態を説明してゆく。図1は、チームデー

タリスト管理装置及びチームデータリスト保管装置を具備した本実施形態のシステム全体の構成を示したブロック図である。同図において、チームデータリスト管理装置30、チームデータリスト保管装置31は以下に詳述するチームデータリスト管理機能、チームデータリスト保管機能をそれぞれ備えており、互いに通信機能を利用してデータを授受している。チームデータリスト管理装置30、チームデータリスト保管装置31は何れもワークステーションなどの一般的なコンピュータで実現することが可能であり、これらコンピュータの主記憶上にはそれぞれチームデータリスト管理機能、チームデータリスト保管機能を実現するためのプログラム（チームデータリスト管理プログラム、チームデータリスト保管プログラム）が記憶される。

【0019】

これらのプログラムはフロッピーディスク、IC（集積回路）カード、光磁気ディスク、CD-ROM（コンパクトディスクー読み取り専用メモリ）等の可搬性のある記憶媒体や、コンピュータに内蔵されるハードディスクなどの大容量の記憶媒体といったコンピュータ読み取り可能な記憶媒体にその一部又は全部が記憶されている。すなわち、当該プログラムは以下に詳述する機能の一部を実現するためのものであっても良く、さらにはコンピュータにすでに記録されているプログラムとの組み合わせでこれら機能を実現できるものであっても良い。そして、チームデータリスト管理装置やチームデータリスト保管装置を作動させるにあたって、これらのプログラムがコンピュータ上のCPU（中央処理装置）の指示の下に予め記憶媒体から主記憶上に転送される。その後、CPUは主記憶上に転送されたプログラムを実行し、それによって装置各部を制御して、以下に詳述する様々な処理を実現している。

【0020】

なお、ここで言う「コンピュータ」にはOS（オペレーティングシステム）や周辺機器等のハードウェアが含まれている。また、コンピュータ読み取り可能な記憶媒体としてはいま述べたようなプログラムを静的に記憶するものに限られるものではなく、専用線や電話回線などの通信回線を通じて短時間だけ動的にプログラムを保持するもの、即ち、インターネット等のネットワークでプログラムや

データを保持、転送、中継するサーバ、ルータ、ゲートウェイといったコンピュータ機器に内蔵された主記憶やキャッシュメモリ、サーバ、クライアントとして機能するコンピュータ内部の揮発性メモリなどのように、一定時間プログラムを保持可能なものをすべて包含している。

【0021】

さて、図1に示すチームデータリスト保管装置31にはハードディスク等のデータベースを構築可能な記憶装置32が接続されている。この記憶装置32は、複数のメンバで構成されるチーム毎にオーソリティデータ33とオーソリティリスト34からなるチームデータリストの組を記憶している。同図では説明の都合からオーソリティデータ33及びオーソリティリスト34の組を一つだけ示しているが、実際にはチームの数だけこれらの組が存在している。ここで、図2(a)，(b)はオーソリティデータ33，オーソリティリスト34の詳細な構造を示したものである。また、同図(c)，(d)はこれ以後に掲げる図面中において、オーソリティデータ33，オーソリティリスト34の記憶内容を簡略化して示すための表記法をそれぞれ示したものである。なお、以下の説明及び図面ではオーソリティデータを「AUD」と略記し、オーソリティリストを「AUL」と略記することがある。

【0022】

オーソリティデータ33は或るチームとその配下のサブチームとの関係を表すデータであって、サブチームとの関係において上位にある当該チームを親チームと呼ぶ。図2(a)に示すように記号“AUD”がオーソリティデータであることを示しており、このオーソリティデータ33は、自身のチームに付与された識別子たるチームID33a，このチームの親チームに付与されたチームIDである親チームID33b，親チームの誰がこのチームを作成したかを意味するチーム作成者33c，このチームに属するメンバの誰に対してチームマスタ権限を与えたかを示すチームマスタ33d，チーム作成者33cのデジタル署名（電子署名とも言う）がなされる署名33eを含んでいる。また、図2(c)において、このオーソリティデータはチーム101のサブチームであるチーム102に関するものであることが分かる。これに加えて、デジタル署名からこのオーソリティ

データのチーム作成者がメンバBであることが分かるほか、チームマスタがメンバXであることが分かる。

【0023】

一方、オーソリティリスト34は各チームにおける複数の管理者を登録したリストであって、当該チームのチームマスタやサブオーソリティに関するデータが含まれている。図2(b)に示すように記号“AUL”がオーソリティリストを意味しており、このオーソリティリスト34はこのチームに関するチームID34a、チームマスタ34b、サブオーソリティ34c(同図の場合は二人)、チームマスタ34bのデジタル署名たる署名34dを含んでいる。そして、図2(d)によれば、チームマスタがメンバXであってその署名がなされているほか、サブオーソリティがメンバC及びメンバDであることが分かる。なお、同図(d)ではチームIDの表記自体は省略されている。以上のように、本実施形態によるチームデータリストは、親チーム及びサブチームの関係を示すリストであるAUDと、サブチーム管理に関わるリストであるAULに分割された構造となっている。

【0024】

なお、オーソリティデータ33やオーソリティリスト34には、図2に示した以外にも、これらデータやリストの作成時間を示すタイムスタンプ、署名33eや署名34dを作成するのに用いられる署名アルゴリズム、オーソリティデータ33やオーソリティリスト34自身の有効期限、オーソリティデータ33やオーソリティリスト34自身の識別番号に関するデータなどを含んでいる。また、メンバ、サブオーソリティ、チームマスタの各個人を識別するためのID(識別子)としては、名前、メールアドレス、組織上の名称、個人のシリアルナンバ、デジタル証明書等、種々のものを用いることが可能である。

【0025】

次に、図3は階層化されたチームの概念図についてその一例を示したものである。同図に示されるように、チームの階層はコンピュータのファイルシステムのように木構造になっており、図中の楕円形がチームを表現するとともに、親チームとそのサブチームが直線で互いに結ばれている。各チームには複数のサブチー

ムを登録することができ、例えば人事部のチームの配下に人事一課、人事二課などのサブチームを登録することが可能になっている。また、頂点に存在するチーム101は木構造の根に相当しているため、ファイルシステム上のルートディレクトリになぞらえて本実施形態では「ルート(Root)」ないしルートチームと呼んでいる。さらに、チーム102及びチーム103は何れもチーム101のサブチームであって、木の上では同じ階層に属するチームである。一方、チーム104はチーム103のサブチームである。

【0026】

一方、図4は図3に示したチーム階層に対応させて各チームのオーソリティリストやオーソリティデータについて具体的な値を記入したものである。なお、同図ではオーソリティリスト及びオーソリティデータの他に、互いに情報や機能を共有する共有メンバの一覧を示したメンバリスト(図中の「ML」)が各チームに含まれている例を示してある。つまり、この図においては、チームデータリストがオーソリティリスト、オーソリティデータ、メンバリストの3種類のリストで構成される。各メンバリスト101m~104mにはメンバリストの作成者の署名とメンバの一覧が図示されているが、これ以外にも、チームの利用目的に合致した様々なチームの管理情報が含まれている。すなわち、各メンバの識別情報、各メンバに付与された公開鍵方式における公開鍵(即ち、所定長のビット列)とこの公開鍵に対応する保有者の識別子(以下、「公開鍵ID」という)、チームID、メンバリストの作成時間を示すタイムスタンプ、チーム内のメンバが利用できる機能(例えば、アプリケーション)に関する情報などが含まれている。このほか、それぞれのメンバリストには各メンバに関する情報として、e-mail(電子メール)アドレスやメンバ自身の住所といった情報も含まれており、これらを用いることで各メンバに関する情報リソースの管理も同時に行うことができる。

【0027】

同図に示す構成によれば、オーソリティデータに記述された親チームIDを辿ってゆくことで、何れのサブチームからもルートたるチーム101に到達することができる。このほか、各チームでは複数の管理者がサブチームを作成可能であ

る。例えばチーム101ではチームマスタA及びサブオーソリティB、Cがサブチームの作成権限を有しており、オーソリティデータ102d、103dの署名から分かるように、サブチームたるチーム102、103はそれぞれチーム101のサブオーソリティB、Cが作成している。

【0028】

あるサブチームのオーソリティデータは当該サブチームの親チームに登録された管理者が作成することになっている。また、当該サブチーム内の誰もが親チームの管理者の指示によってこのサブチームのチームマスタになることができる。例えばチーム104では、オーソリティデータ104dのデジタル署名がメンバVであるから、親であるチーム103の管理者の一人であるサブオーソリティVがオーソリティデータ104dを作成しており、チーム104のチームマスタとしてメンバLを指名している。

【0029】

一方、オーソリティリストは各チームのチームマスタが作成して署名することになっている。例えば、チーム103のオーソリティリスト103uはチームマスタたるメンバXが作成したものであって、そこにはメンバXのデジタル署名がなされている。そのため、オーソリティリスト103u中のサブオーソリティに関するデータはメンバXのみが管理できることになり、親チームたるチーム101の管理者（即ち、チームマスタAやサブオーソリティB、C）の干渉を受けることはない。換言するならば、オーソリティリストの署名者をチームの作成者（即ち、親チームのチームマスタやサブオーソリティ）にしてしまうと、例えば人事部長が人事課長に課内部の管理を任せることができなくなって自分で管理してゆかねばならなくなる。同様にして、メンバリストの署名についても各チームのチームマスタが行うことから、各チーム内の共有メンバに関する管理についても親チームの干渉を受けずに済むことになる。例えばチーム103のメンバリスト103mはチームマスタXが署名しているため、親チームの管理者が管理することはできない。ただし、サブチームを最初に作成したときの初期状態や、サブチームのチームマスタを親チームのチームマスタやサブオーソリティが変更した場合には、オーソリティリストの署名は、該サブチームを作成した親チームのチー

ムマスタ又はサブオーソリティの署名となっている。

【0030】

以上の点をまとめると、本実施形態ではオーソリティデータとオーソリティリストを分離する構成としており、親チームはサブチームのオーソリティデータAUDを参照することができる一方、親チームの管理者がオーソリティリストやメンバーリストを改竄できないようにすることで、サブチーム内部の管理に親チームは関与しないようにしている。これによって、各チームのチームマスタは、自分でサブオーソリティを選択できるほか、チーム内の情報共有のメンバ管理も行うことができる。

【0031】

次に、図1のチームデータリスト保管装置31において、権限確認機能35はクライアントCL側からオーソリティデータ33やオーソリティリスト34に対する参照、変更、削除の各要求があったときに、要求者を識別してこれらの要求を許可するのか拒否するのかを判断する。この判断にあたっては、要求対象となっているチームのチームマスタ、サブオーソリティや当該チームの親チームやサブチームとの間の関係のほか、チームに所属するメンバ等の権限と要求者本人に与えられている権限などを照らし合わせている。つまり、要求内容によって判断手順の詳細が異なるためその詳細については後述する動作説明に譲る。次に、リスト保管機能36は権限確認機能35がオーソリティデータ33やオーソリティリスト34を使用するにあたって、これらのリストを記憶装置32から取得し、記憶装置32から削除し、あるいは記憶装置32へ保存する処理を司っている。以下の説明では、権限確認機能35がオーソリティデータ33やオーソリティリスト34にアクセスする場合には必ずリスト保管機能36が介在することを前提としているが、煩雑になるため一々説明しない。

【0032】

次に、チームデータリスト管理装置30において、リスト正当性確認機能37はルートチームに至るまで親チームのオーソリティリスト及びオーソリティデータを順次辿ってゆき、最終的にチーム101のチームマスタAの署名を確認してオーソリティリスト及びオーソリティデータの正当性を検証している。なお、こ

ここで言う正当性とは改竄や越権行為などが無く正当な手順を経てチーム階層の管理が行われていることを意味している。次に、AUD・AUL変更機能38は、リスト正当性確認機能37が取得したオーソリティデータ33やオーソリティリスト34に対してメンバや管理者の追加、削除、置換などの変更を加えるほか、サブチーム作成時などではオーソリティデータ33及びオーソリティリスト34を新たに作成することもある。次いで、電子署名機能39はAUD・AUL変更機能38によって処理がなされたオーソリティデータ33やオーソリティリスト34に対し、変更者本人しか知り得ない秘密鍵ないし署名鍵を用いた暗号とハッシュ関数とを併用してこれらリストの作成者ないしは変更者（即ち、チームマスタ又はサブオーソリティ）のデジタル署名を付加する。

【0033】

次に、公開鍵管理機能40は、チームデータリスト管理装置30に接続された公開鍵データベース41にアクセスして、公開鍵と当該公開鍵に対応する公開鍵IDを取得する。ちなみに、実際の形態において、公開鍵データベース41はチームデータリスト管理装置30に直接的に接続されたローカルな形態のみならず、インターネット等のネットワーク上に設置されたサーバ（例えば、認証局）に存在している形態も当然に考えられる。こうした形態によれば、公開鍵管理機能40は認証局上に登録されたホームページを介して公開鍵データベース41にアクセスし、そこから上述した公開鍵及び公開鍵IDをファイルの形式で取得することも可能となる。

【0034】

次に、上記構成によるチームデータリスト管理装置30およびチームデータリスト保管装置31を有するシステムの動作についてクライアントCLからサーバSVに対して為される要求内容毎に説明してゆく。

【0035】

〔サブチームの作成〕

図5はサブチームを作成するための処理手順を示している。ここでは図4に示したチーム101のサブオーソリティであるメンバCが、チーム101の配下にチームマスタをメンバXとしたサブチーム103を作成するものとする。これは

、人事部長の代行として部長代理が人事部の下に課を新設する業務を遂行する場合などに相当する。ここで、チームデータリスト保管装置31では正当な手順に従って作成されたチーム101に関するチームデータリストが予め記憶装置32上に格納されており、ルートチーム101のチームマスタAによる管理体系でサブチームの作成が行われる。なお、図4に示したように、チーム101には親チームは存在しないのでオーソリティデータ101dの親チームIDには固定値「Root」が設定されているほか、チームマスタはメンバAであるためオーソリティデータ101d及びオーソリティリスト101uには何れもメンバAのデジタル署名がされている。もっとも、ルートチームには仮想的に「Root」という親チームがあると見なすことができ、また、この親チームがチームマスタとしてメンバAを指名しているから見なすことができる。

【0036】

まず、メンバCからのサブチーム作成指示に従って、チームデータリスト管理装置30がサブチーム作成要求をチームデータリスト保管装置31に送出する（ステップS11）。チームデータリスト保管装置31は記憶装置32からオーソリティデータ101d及びオーソリティリスト101uを取得して、これらをチームデータリスト管理装置30に送出する。その際、チームデータリスト保管装置31はチーム101の配下にサブチーム（即ち、図4に示すチーム102）があればそれらチームに関するチームデータリストも併せてチームデータリスト管理装置30へ送出する（ステップS12）。チームデータリスト管理装置30では、AUD・AUL変更機能38がメンバCからの指示に基づいて、親チームIDをチーム101、チームIDをチーム103、チームマスタをメンバXとしたオーソリティデータ103dを作成するとともに、チームマスタをメンバXとしたオーソリティリスト103uaを作成する。次に、AUD・AUL変更機能38は作成したオーソリティリスト103uaをオーソリティデータ103dと一緒にして電子署名機能39に引き渡す。

【0037】

電子署名機能39は、秘密鍵ファイルや秘密鍵の記録されたICカード等からメンバCに関する秘密鍵を取得し、これを基にAUD・AUL変更機能38から

送られたオーソリティデータ 103 d 及びオーソリティリスト 103 u a に対して要求者たるメンバ C のデジタル署名を行う。この時点ではオーソリティリスト 103 u a の署名はチームマスタ X のものではなく、サブチーム作成者の署名になっている（以上、ステップ S 13）。次に、電子署名機能 39 は、チーム 103 について作成されたオーソリティデータ 103 d 及びオーソリティリスト 103 u a をチームデータリスト保管装置 31 に送出して、これらの保存要求を行う（ステップ S 14）。

【0038】

チームデータリスト保管装置 31 では、権限確認機能 35 が図 6 のフローチャートに示される権限確認を行う。まず、権限確認機能 35 は保存要求を行った要求者がメンバ C であることを識別（ステップ S 31）し、チーム 101 に関するオーソリティデータ 101 d 及びオーソリティリスト 101 u を基に、メンバ C がチーム 101 のチームマスタ又はサブオーソリティであるかどうか調べる（ステップ S 32）。この場合、メンバ C はチーム 101 のサブオーソリティであるため、正当な権限を持つ者によって作成されたデータの保存要求と判断（同ステップの判断結果が“YES”）する。ちなみに、同ステップの判断結果が“NO”となる場合には改竄ないしは不正行為が存在しているため、権限確認機能 35 は要求された保存動作を行うことなく処理を中止する。

【0039】

次に、権限確認機能 35 は作成されたサブチーム 103 のオーソリティデータ 103 d 及びオーソリティリスト 103 u a の署名がともに要求者たるメンバ C のものであることを確認する（ステップ S 33）。この場合は、前述したように何れもメンバ C が署名しているため同ステップの判断結果は“YES”となり、権限確認機能 35 は正常な権限でサブチームが作成されたものと最終的に判断して、作成されたサブチームのオーソリティデータ 103 d とオーソリティリスト 103 u a を記憶装置 32 に保存する（ステップ S 34）。ちなみに、ステップ S 33 の判断結果が“NO”となる場合には改竄ないしは不正行為が存在しているため、権限確認機能 35 は要求された保存動作を行うことなく処理を中止する（なお、以上の処理は図 5 のステップ S 15 に相当）。以上の手順によってサブ

チームの作成が完了する。

【0040】

この後、チーム103のチームマスタたるメンバXから当該チームに対して、情報共有のメンバやサブチーム作成権限者の設定といった管理要求があったものとする。なお、ここでは一事例としてチーム103のサブオーソリティとしてメンバW及びメンバVを新たに登録する場合について説明する。図5に示すように、まずチームデータリスト管理装置30は、メンバXから指示された管理要求に基づいて、親チーム103に関するチームデータリストをチームデータリスト保管装置31に要求する（ステップS16）。すると、チームデータリスト保管装置31は要求内容をもとにしてサブチーム103のほかルートチームに至るまでの全ての親チーム（この場合はルートチームたるチーム101のみ）に関するチームデータリストをそれぞれチームデータリスト管理装置30側に転送する（ステップS17）。チームデータリスト管理装置30では、リスト正当性確認機能37が図7のフローチャートに示される処理手順に従って、転送されてきたリストの正当性を調べる（ステップS18）。

【0041】

まず、リスト正当性確認機能37は、管理対象であるチーム103のオーソリティデータ103d及びオーソリティリスト103uaのデジタル署名を参照してそれらが改竄されているかどうか確認（ステップS41）し、改竄があれば不正行為があったものとして管理要求に関わる処理を中止する（同ステップの判断結果が“NO”）。一方、同ステップの判断結果が“YES”であって改竄がなければ、リスト正当性確認機能37は、オーソリティデータ103dからメンバXがチーム103のチームマスタであることを確認できる。ここで、通常であれば、リスト正当性確認機能37はオーソリティリスト103uaからその署名者がチームマスタたるメンバXであることを確認する。しかし、前述したようにこの時点はサブチーム作成途上の過渡期になっており、オーソリティリスト103uaの署名者がサブチーム作成者であるメンバCになっているので、メンバCがサブチームを作成する正当な権利を持っているかどうかは、後述する処理（ステップS45）で、メンバCが親チーム101のチームマスタもしくはサブオーソ

リティとして登録されているか調べることで確認する（ステップS42）。

【0042】

次に、リスト正当性確認機能37はオーソリティデータ103dの親チームIDから親チームがチーム101であることを知り（ステップS43）、親チームのオーソリティデータ101d及びオーソリティリスト101uのデジタル署名が改竄されているかどうか調べる（ステップS44）。そしてこれらの何れかでも改竄されていれば、不正行為があったとしてリスト正当性確認機能37は処理を中止する（同ステップの判断結果が“NO”）が、同ステップの判断結果が“YES”であって改竄がなければ、引き続いてチーム103の作成者が親チームのチームマスタ又はサブオーソリティであるかどうかを確認する（ステップS45）。この場合、チーム103のオーソリティデータ103dの署名者はメンバCであり、また、親であるチーム101のオーソリティリスト101uからメンバCが親チームのサブオーソリティとして登録されていることが分かり、チーム103が正当な作成権限を持つ者によって作成されていることが確認できる（同ステップの判断結果が“YES”）。なお、同ステップの判断結果が“NO”であれば、リスト正当性確認機能37は不正行為があったものとして処理を中止する。

【0043】

次に、リスト正当性確認機能37は親であるチーム101がルートであるかどうか調べるが、この場合はチーム101のオーソリティデータ101dの親チームIDが“Root”であることからルートチームであることが分かる（ステップS46の判断結果が“YES”）。そこで、リスト正当性確認機能37はチーム101のオーソリティデータ101dを調べることでそのチームマスタがメンバAであることが分かる。そして、このメンバAによってオーソリティデータ101d及びオーソリティリスト101uが署名されていることから、チーム階層がチームマスタAの下で正当に管理されていることを確認できる（ステップS47）。最後に、メンバX自身がチームデータリスト管理装置30を操作して、ルートチーム101のチームマスタAが管理するチーム階層の下に、情報共有などのチームデータリストの利用や階層化されたチームの利用が為されていることを

承認して、この旨をリスト正当性確認機能37に通知する。

【0044】

以上の手順により、リスト正当性確認機能37は、チーム101のチームマスタAの指名したサブオーソリティCがチーム103に関するオーソリティデータ及びオーソリティリストを作成しており、チームデータリスト保管装置31から正常な状態でこれらチームデータリストが取得されていることを確認できる。そこで、リスト正当性確認機能37はチームデータリスト保管装置31から転送されたチームデータリストをAUD・AUL変更機能38に渡す。なお、図7のステップS46で親チームがルートチームと判断されなかった場合、例えばチーム103のサブチームであるチーム104に対して管理要求を行った場合、リスト正当性確認機能37は対象とするチームを親チームに変更してチーム階層をルートチームに向かって一つ上がり（ステップS49）、親チームがルートチームたるチーム101になる（ステップS46の判断結果が“YES”）までステップS42～S46及びステップS49から成るループを繰り返して実行する。

【0045】

次に、AUD・AUL変更機能38はチーム103のオーソリティリスト103uaに対して、サブオーソリティとしてメンバW及びメンバVを加えたオーソリティリスト103uを作成し、これをオーソリティデータ103dとともに電子署名機能39に渡す。電子署名機能39は前述した秘密鍵ファイル等からチームマスタXに関する秘密鍵を取得し、渡されたオーソリティリスト103uに対してチームマスタXの署名を行ったのち（以上、ステップS19）、これをオーソリティデータ103dとともにチームデータリスト保管装置31に転送してこれらチームデータリストに関する保存要求を行う（ステップS20）。

【0046】

チームデータリスト保管装置31において、権限確認機能35はチームデータリスト管理装置30からの保存要求に対し、記憶装置32に保管されているチーム101に関わるチームデータリストとクライアント側から転送されてくるチーム103に関わるチームデータリストに基づいて、図8のフローチャートで示される権限確認を行う。すなわち、まず権限確認機能35は保存要求を指示した要

求者がメンバXであることを識別（ステップS51）し、転送されてきたオーソリティデータ103d及びオーソリティリスト103uをもとにして、上記要求者が、チーム103のチームマスタ、親であるチーム101のチームマスタ又はサブオーソリティの三者のうち何れかに一致するかどうかを確認する。この場合は要求者たるメンバXがチーム103のチームマスタとして登録されている（ステップS52の判断結果が“YES”）ので、権限確認機能35は要求者が保存要求に対する正当な権限を持っていると判断する。ちなみに、同ステップの判断結果が“NO”であれば、権限確認機能35は要求者に正当な権限が与えられていないものとして処理を中止する。

【0047】

次に、権限確認機能35はオーソリティデータ103dの署名者が親チームのチームマスタ又はサブオーソリティの何れかに一致するかどうか確認する。この場合、オーソリティデータ103dの署名者はメンバCであって親チーム101のサブオーソリティである（ステップS53の判断結果が“YES”）ため、権限確認機能35は要求者が保存要求に対する正当な権限を持っていると判断する。ちなみに、同ステップの判断結果が“NO”であれば、権限確認機能35は改竄や不正行為があったものとして処理を中止する。次に、権限確認機能35は、オーソリティリスト103uの署名者がオーソリティデータ103dに登録されているチームマスタと一致するかどうかを確認する。この場合、オーソリティリスト103uの署名者はオーソリティデータ103dの示すチームマスタXである（ステップS54の判断結果が“YES”）ことから、権限確認機能35は正常な権限を持つ者によってチーム103が作成されたものと最終判断を下して、チームデータリスト管理装置30から転送されたチームデータリストを記憶装置32に保存して、チーム103に関するチームデータリストの内容を更新する（ステップS55）。なお、ステップS54の判断結果が“NO”であったならば、権限確認機能35は改竄や不正行為があったものとして処理を中止し、上述したステップS55における保存処理は実施しない。

【0048】

以上のようにして、サーバSV側に保管されているチームデータリストに基づ

いて、メンバXが間違いなくルートチームのチームマスタAによる管理体系の中で正当にチーム103のチームマスタとして任命されていることが検証できる（図5のステップS21）。

【0049】

〈サブチームのチームマスタの変更〉

次に、サブチームのチームマスタを変更するための処理手順について図9を参照して説明する。ここではルートたるチーム101にサブオーソリティとして登録されているメンバBが、サブチームであるチーム103のチームマスタをメンバXからメンバZへ変更する場合を例に挙げることにする。これは人事一課長が異動になったために、人事部長の代わりに部長代理が課長を変更する場合などに相当する。まず、チームデータリスト管理装置30はサブチーム103に関わるチームデータリストの変更要求をチームデータリスト保管装置31に送出する（ステップS61）。これにより、チームデータリスト保管装置31は図5のステップS12と同様にチーム101とその配下のサブチームに関するチームデータリストをチームデータリスト管理装置30側に転送する（ステップS62）。

【0050】

チームデータリスト管理装置30では、リスト正当性確認機能37が図7で説明した処理手順に従って転送されてきたチームデータリストの正当性の検証を行い（ステップS63）、その正当性が検証できた場合に転送されてきたチームデータリストをAUD・AUL変更機能38に引き渡す。AUD・AUL変更機能38は、メンバBからの指示内容に従って、引き渡されたチームデータリストのうちオーソリティデータ103dについてチームマスタをメンバXからメンバZに変更して、この変更されたオーソリティデータと引き渡されたオーソリティリストとを電子署名機能39に送る。電子署名機能39は送られたチームデータリストに対してそれぞれ前述した秘密鍵ファイル等からメンバBに関する秘密鍵を取得してデジタル署名を施し、それによってオーソリティデータ103db及びオーソリティリスト103ubを作成（ステップS64）したのち、これらチームデータリストをチームデータリスト保管装置31に転送して保存要求を行う（ステップS65）。

【0051】

チームデータリスト保管装置31では、権限確認機能35が転送されてきたチームデータリストを基に図8に示した手順に従った権限確認を行って、その正当性が確認された場合に、転送されてきたチームデータリストを記憶装置32に保存する。ここで、サブチーム作成時（図5のステップS21）と相違する点は、チームマスタ変更処理においてはオーソリティリスト103ubの署名者であるメンバBとオーソリティデータ103dbで指名されているチームマスタたるメンバZが異なっていることである（ステップS54の判断結果が“NO”となるケース）。そこでこの場合、権限確認機能35はオーソリティリスト103ubの署名者が親チームに登録された管理者たるチームマスタA、サブオーソリティB、サブオーソリティCの何れかに一致していれば、正当な権限を持つ者による署名であると判断する。そして以上のようにして、サーバSV側にはチーム103に関わるチームデータリストとして作成時間の異なる2組のオーソリティリスト及びオーソリティデータ、即ちチームマスタ変更前後の各チームデータリストが保存される。その後、チームデータリスト保管装置31は、チーム103の新たなチームマスタであるメンバZの署名をオーソリティリスト103ubに付与するために、オーソリティデータ103db及びオーソリティリスト103ubをチームデータリスト管理装置30に転送する（ステップS66）。

【0052】

チームデータリスト管理装置30では、リスト正当性確認機能37が図7の処理手順に従って、転送されてくるチームデータリストの正当性を検証したのち、これをAUD・AUL変更機能38を介して電子署名機能39に渡す。電子署名機能39は、前述した秘密鍵ファイル等からメンバZに関する秘密鍵を取得し、これを基にオーソリティリスト103ubに対してメンバZのデジタル署名を行ってオーソリティリスト103ucを作成する（ステップS67）。次いで、電子署名機能39は作成されたオーソリティリスト103ucをオーソリティデータ103dbとともにチームデータリスト保管装置31に転送する（ステップS68）。チームデータリスト保管装置31では、権限確認機能35が転送されてきたチームデータリストを基に図8の処理手順に従って権限確認を行い、その正

当性が確認された場合に転送されてきたチームデータリストを記憶装置32に保存して、チーム103に関わるチームデータリストの更新処理を行う。以上によって、チームマスタが正常な手順を踏んで変更されたことになる。

【0053】

〈サブオーソリティの変更〉

次に、サブオーソリティを変更するための処理手順について図10を参照して説明する。ここでは、ルートであるチーム101のチームマスタAが、このチーム101でサブオーソリティとして登録されているメンバBの作成権限を剥奪する場合を例に挙げて説明する。これは、部長代理が異動になるなどして、人事部長がこの部長代理を人事部から除外する場合などに相当する。なお、同図では図9に示したチームマスタ変更によってサブオーソリティBが作成者となっているチーム103を前提としている。また、同図では、サブオーソリティBの作成権限が削除されるのに伴ってチーム103を削除してしまう場合と、チーム103を継続させる場合の2つのケースを併せて図示してある。したがって、メンバAがチームデータリスト管理装置30に対して要求を指示する場合にはチーム103を存続させるのかの可否をも併せて指示するようにしている。

【0054】

まず、チームデータリスト管理装置30はチーム101に登録されているサブオーソリティBに対する変更要求（削除要求）をチームデータリスト保管装置31に対して送出する（ステップS71）。これにより、チームデータリスト保管装置31はチーム101の配下にあるサブチームのオーソリティデータを参照して、それらサブチームの中からサブチームBが作成者となっているチーム103を検索したのち、チーム101とチーム103に関するチームデータリストをチームデータリスト管理装置30側に転送する（ステップS72）。チームデータリスト管理装置30では、リスト正当性確認機能37が図7で説明した処理手順に従って、転送されてきたチームデータリストの正当性の検証を行い、その正当性が検証できた場合に転送されてきたチームデータリストをAUD・AUL変更機能38に引き渡す。

【0055】

AUD・AUL変更機能38はメンバAからの指示内容に基づいて、引き渡されたチームデータリストのうち、オーソリティリスト101uに記述されているサブオーソリティの中からメンバBを削除したオーソリティリスト101ubを作成する（ステップS73）。これに加えて、AUD・AUL変更機能38はオーソリティデータ103dbに付与されているメンバBの署名を削除してオーソリティデータ103dcを作成する（ステップS74）。この後、AUD・AUL変更機能38はオーソリティデータ103dcとオーソリティリスト103ucを電子署名機能39に送出する。

【0056】

電子署名機能39はメンバAからの指示内容に従って以下の2通りの処理の何れかを行う。第1に、チーム103を継続させる要求が来ているのであれば、電子署名機能39はチーム103の存在をメンバAが承認したものと見なし、前述した秘密鍵ファイル等からメンバAに関する秘密鍵を取得し、これを基にオーソリティデータ103dcにメンバAの署名を添付してオーソリティデータ103ddを作成する（ステップS75）。次いで、電子署名機能39はオーソリティデータ101d、103dd及びオーソリティリスト101ub、103ucをチームデータリスト保管装置31に転送してこれらチームデータリストの保存要求を行う（ステップS76）。チームデータリスト保管装置31では、権限確認機能35が転送されてきたチームデータリストを基に図8に示した手順に従った権限確認を行って、その正当性が確認された場合に、転送されたチームデータリストで記憶装置32の内容を更新する（ステップS77）。

【0057】

第2に、チーム103を消去する旨の要求が来ているのであれば、電子署名機能39はチーム101に関するチームデータリスト、すなわちオーソリティデータ101d及びオーソリティリスト101ubをチームデータリスト保管装置31へ転送するとともに、チーム103を無効にする旨の命令をチームデータリスト保管装置31に送出する（ステップS78）。チームデータリスト保管装置31では、権限確認機能35が記憶装置32に保存されているオーソリティリスト101uと送られてきたオーソリティリスト101ubを照合することでサブオ

ーソリティBの削除を認識することができる。これに加えて、権限確認機能35はオーソリティデータ101d及びオーソリティリスト101ubの内容から、チームマスタがメンバAであって且つこれらチームデータリストが何れもこのメンバAによってデジタル署名されていることが分かる。こうしたことから、権限確認機能35はチームマスタAが正当な権限でサブオーソリティBを削除したものと判断して、オーソリティデータ101d及びオーソリティリスト101ubの内容で記憶装置32中のチーム101のチームデータリストを更新する。次いで、権限確認機能35は記憶装置32上からチーム103に関わるオーソリティデータ及びオーソリティリストを削除する（以上、ステップS79）。以上によって、サブオーソリティBの作成権限がサーバSV上のチームデータリストから削除されたことになる。

【0058】

＜サブチームの削除＞

次に、サブチームを削除するための処理手順について図11を参照して説明する。ここでは、ルートであるチーム101にサブオーソリティとして登録されているメンバCが、前述した図5の処理手順で作成したチーム103を削除する場合を例に挙げて説明する。これは、人事部の下にある人事一課が廃止されたために、人事部長代理が課の廃止に関わる業務を行う場合などに相当する。ここで、メンバCは、サブチームであるチーム103の親に相当するチーム101のサブオーソリティの権限でもってチーム103を削除するため、自分が間違いなくメンバC本人であることをチームデータリスト保管装置31に対して証明してやる必要がある。そのため、チームデータリスト管理装置30は後述するようにチームデータリスト保管装置31に対してメンバCの電子署名を通知するようにしている。

【0059】

さて、まずメンバCがチームデータリスト管理装置30に対してチーム103の削除指示を行うと、チームデータリスト管理装置30は電子署名機能39によってメンバCの電子署名を作成したのち、チーム103をメンバCの権限で削除する旨の命令とメンバCの電子署名を組にしてチームデータリスト保管装置31

へ転送する（ステップS81）。なお、電子署名を添付する以外の方法として、削除命令の転送時に証明する「シェイクハンド」あるいは「チャレンジレスポンス」と呼ばれる方法（詳細は後述）を採用することも考えられるが、ここでは電子署名を用いた方法に沿って説明を行うものとして、最後にシェイクハンドについて説明することとする。

【0060】

チームデータリスト保管装置31がチームデータリスト管理装置30からチーム103の削除命令を受け取ると、権限確認機能35はチーム101及びチーム103に関するチームデータリストを参照して、チーム101に登録されているサブオーソリティCがチーム103の作成者であることを知る。また、権限確認機能35はオーソリティデータ103dに記述されたメンバCの署名と削除命令に添付されているメンバCの署名を照合して、これらが一致していることことを確認することにより、削除を指示した者が間違いなくメンバC本人であることについて確証を持てる。こうして、権限確認機能35は正当な権限で発行された削除命令であるものと判断して、記憶装置32上からチーム103に関するオーソリティデータ103d及びオーソリティリスト103uを削除する（以上、ステップS82）。以上によって、サブオーソリティCによるチーム103の削除処理が完了したことになる。

【0061】

ところで、メンバAはチーム101のチームマスタであることから、サブオーソリティCの代わりにサブチームたるチーム103を削除する正当な権限を有している。この場合に、メンバAがチームデータリスト管理装置30に対してチーム103の削除指示を行うと、チームデータリスト管理装置30は電子署名機能39によってメンバAの電子署名を作成して、チーム103をチームマスタAの権限で削除する旨の命令とメンバAの電子署名をチームデータリスト保管装置31へ転送する（ステップS83）。チームデータリスト保管装置31において、権限確認機能35はチーム101及びチーム103に関するチームデータリストを参照することで、チーム101に登録されているサブオーソリティCがチーム103の作成者であり、且つ、このサブオーソリティCは親チーム101のチー

ムマスタAによってサブオーソリティとして指名されたものであることが分かる。また、権限確認機能35はオーソリティデータ101dに記載されているメンバAの署名と削除命令に添付されているメンバAの署名を照合することで、削除を指示した者が間違いなくメンバA本人であることを確認する。こうして、権限確認機能35は正当な権限で発行された削除命令であるものと判断して、記憶装置32上からチーム103に関するオーソリティデータ103d及びオーソリティリスト103uを削除する（以上、ステップS84）。

【0062】

以上によって、チームマスタAによるチーム103の削除処理が完了したことになる。なお、上述したメンバ以外にも、例えばチーム101にサブオーソリティとして登録されているメンバBがサブチームであるチーム103を削除することも可能である。

【0063】

最後に、図12を参照しつつ、上述したシェイクハンドないしチャレンジレスポンスの処理手順の詳細を説明する。まず、クライアントCLはサーバSVにアクセスする際にユーザ（図11の場合で言えばメンバCまたはメンバA）のユーザ名およびユーザ公開鍵をサーバSVに送付する（ステップS101）。サーバSVは乱数を発生させて内部に記憶するとともにこの乱数をユーザ公開鍵で暗号化（ステップS102）し、暗号化されたデータを「チャレンジデータ」としてクライアントCLに送信する（ステップS103）。クライアントCLはサーバSVから送られたチャレンジデータをユーザ公開鍵に対応した秘密鍵で復号化（ステップS104）し、得られた復号化データを「チャレンジレスポンス」としてサーバSVに返送する（ステップS105）。サーバSVはクライアントCLから送られたチャレンジレスポンスとステップS102で発生させた乱数とを比較して通信相手を確認する。すなわち、両者が一致すればステップS101で送付されたユーザ公開鍵に対応する秘密鍵を知っている者が通信相手であることを確認（認証成功）することができる。これに対し、両者が不一致であれば通信相手が正当な権限を持った者でない可能性のある（認証失敗）ことがわかる（以上、ステップS106）。この後、サーバSVはステップS106で得られた確認

結果（認証成功または認証失敗）をクライアントCLに通知する（ステップS107）。以上のようにすることで、電子署名を添付した場合と同じく、メンバCやメンバAが本人であることをサーバSV側で確かめることができる。

【0064】

なお、クライアントCLからサーバSVへユーザ公開鍵を送る代わりに「ユーザ公開鍵番号」を送るようにしても良い。ここで言うユーザ公開鍵番号はユーザ本人を識別・認証するための情報であって、各ユーザ公開鍵に予め付与されているシリアル番号のことである。さらに詳しく説明すると、ユーザ公開鍵番号はユーザ公開鍵を一意に識別するための各ユーザ公開鍵に対応した情報であって、例えば、上述した認証局から発行された証明書に含まれている当該証明書のシリアル番号である。また、ユーザ本人を識別・認証するための情報としては、いま述べたユーザ公開鍵番号以外にも、実際に鍵作成者本人を識別するIDや名前などの様々な情報を利用することができる。

【0065】

〔第2実施形態〕

図13は本実施形態によるチームの階層化について示したものであって、チーム内のメンバの利用できるアプリケーションがチーム毎に異なる形態を実現したものである。同図では、図4に示したチームのうちチーム101～103に対応するものだけを示してある。オーソリティリスト及びオーソリティデータに関しては図4に示したものと同一であるが、このほか、各チームにはメンバリストの代わりにメンバリストの内容を包含するアプリケーションリスト101a、102a、103aが設けられている。すなわち、これらアプリケーションリストには、各チームに属するメンバの利用可能なシステムのほか、そのチームに属するメンバの一覧が記載されている。アプリケーションについては例えばチーム101のアプリケーションリスト101aには人事管理システム、経理システム、スケジュール、ファイル共有システムが登録されている。また、メンバー一覧については図4のメンバリストに記載されているものと同じである。

【0066】

この第2実施形態では、第1実施形態と同様にチームの生成に関しては親チー

ムの干渉を受けるものの、アプリケーションリストは各チームのチームマスタがそれぞれ署名するので、チーム内の管理は親チームからの干渉を受けずに行うことができる。つまり、チーム内で利用可能なアプリケーションをどのメンバで共同利用するかといったことは、チームマスタが親チームの管理者から独立して行うことができる。例えば、チーム101のサブチームであるチーム102では、アプリケーションリスト102aの署名はチーム102のチームマスタであるメンバYが署名しており、チーム101の管理者であるチームマスタAやサブオーソリティB、Cの干渉を受けなくて済む。

【0067】

〔第3実施形態〕

本実施形態では、サブチームを管理するという観点から見たメンバ、サブオーソリティ、チームマスタという上述の権限分担に加えて、情報を共有してゆくためのチーム内での管理権限分担として各チームに属する者をメンバ、サブマスタ、チームマスタの3種類に分類している。このうち、サブマスタはチームマスタによって指名されたチーム内の管理者であって、チームマスタやサブマスタを変更することは許されていないが、一般のメンバについて追加、削除、変更を行うことのできる者である。一方、チームマスタはサブマスタ又はメンバの変更を行えるほか、自身のチームマスタでさえ変更することのできる者である。他方、サブマスタ及びチームマスタ以外の一般のメンバはメンバに提供される情報や機能を共有する者であって、チームデータリストの内容に変更を加える等の権限はいっさい与えられていない。なお、サブマスタやチームマスタも特別な権限が与えられてはいるが、チーム内のメンバであることに変わりはなく、その意味でサブマスタ又はチームマスタをメンバと呼ぶことがある。

【0068】

図14は本実施形態におけるチームの階層化について示したものである。同図では、図4に示した第1実施形態の各チームに対してさらにチームマスタリストを加えてある。こうすることで、チーム毎に情報共有を管理するとともに、各チーム内の情報共有のメンバの管理を複数の管理者が行えるようにしている。図14において、チームマスタリスト101t~104tは各チームに登録されてい

るチームマスタ及びサブマスタの一覧とチームマスタの署名が記載されている。もっとも、これ以外にもチームマスタリストには、チームマスタ又はサブマスタの識別情報、公開鍵、公開鍵ID、チームID、チームマスタリストの作成時間を示すタイムスタンプなどが含まれている。このほか、チームマスタリスト34には、チームに関する情報としてチームのメンバ数、チームの作成された時間、チーム内の各メンバが利用することのできる各種機能などの情報（例えば、上述したアプリケーションリスト）も含まれており、これらを用いることで各チームに関する情報リソースの管理を同時に行うことができる。

【0069】

チームマスタリストの署名は、各チームのチームマスタがチーム作成時に署名し、以後はずっとチームマスタの署名になっている。これに対し、メンバリストについては各チーム内のチームマスタの他に、サブマスタがこれを管理する権限を付与されているため、チームマスタ以外にサブマスタの署名が為されている場合もある。例えば、メンバリスト101maに関してはチーム101のサブマスタとして登録されているメンバBの署名がなされている。一方、チーム102のように、チームマスタリスト102tにサブマスタが登録されていない場合にはメンバリスト102maはチームマスタであるメンバBが署名することになる。

【0070】

この図14ではサブチームの管理権限、メンバの管理権限をそれぞれオーソリティリスト／オーソリティデータ、チームマスタリストに分割しているため、各チーム内でサブオーソリティとサブマスタに異なる者を割り当てることができる。例えば、チーム103ではメンバW及びメンバVがサブオーソリティであり、メンバY及びメンバZがサブマスタであるため、サブチームの管理とメンバ管理を異なる者が担当して負荷分散を図ることもできる。もっとも、実際にはサブオーソリティとサブマスタを同じメンバにできてしまっても良い。その場合はオーソリティリストとメンバリストを統合して一つのリストにしてしまうことが可能となる。

【0071】

〔第4実施形態〕

上述した各実施形態では、チームデータリストを使用する都度、チームマスタが間違いなく自分のチームマスタであるかどうかをユーザがクライアントCL側で確認する必要がある。例えば、チームデータリスト管理装置30を構成するコンピュータのディスプレイ上に、“このリストは以下のメンバが管理者となって正常に管理されています。名前：メンバA。組織：三菱マテリアル株式会社。作業を続行する場合はOKボタンをマウスでクリックして下さい”などといったメッセージが表示される。このように、ユーザは当該メッセージを目視で確認する必要が生じてくるため、ユーザに対して煩わしい印象を与える可能性がないとは言えない。こうした点を改善するには以下の機能をリスト正当性確認機能37と連携する新たな機能として追加し、あるいは、リスト正当性確認機能37の一機能として組み込むようにすることで解決される。

【0072】

すなわち、ルートチーム101におけるチームマスタの公開鍵をチーム毎に予めクライアントCL側の例えば公開鍵データベース41（図1参照）に登録しておき、公開鍵管理機能40が公開鍵データベース41からチーム101のチームマスタに関する公開鍵を取得してこれをリスト正当性確認機能37に通知する。もしくは、公開鍵データベース41には公開鍵に関する情報として公開鍵を識別するためのシリアル番号等を登録しておき、公開鍵管理機能40がこのシリアル番号を公開鍵データベース41から取得したのち、これをもとにチームデータリスト管理装置30の外部（例えばインターネット上）に登録されている公開鍵を別途取得してリスト正当性確認機能37に渡すように構成しても良い。

【0073】

一方、リスト正当性確認機能37は、コンピュータのディスプレイ上に上述したようなメッセージを出す代わりに、公開鍵管理機能40から通知されるチーム101のチームマスタの公開鍵に基づいて、チームデータリスト保管装置31から転送されてくるオーソリティデータ101dに含まれているチームマスタのデジタル署名を確認するようにして、当該署名が登録されているチームマスタのものかどうかを判断する。こうすることで、ユーザがディスプレイ上の表示をもとに目視で確認することなく、ルートチーム101のチームマスタの正当性を検証

できるようになる。

なお、チームマスタを確認するための情報としては公開鍵以外にも様々な情報を利用できるのはもちろんである。

【0074】

以上の通り、チームを階層化するためのチームデータリストを管理するチームデータリスト管理プログラムを記録した記録媒体において、チームデータリスト管理プログラムは、（１）所定の要求先に前記チームデータリストの操作要求を行う処理と、（２）前記操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストを有するチームデータリストを前記要求先から取得する処理と、（３）前記識別子を用いて取得された各チームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストの電子署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者による署名であることを確認したのち、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認処理と、（４）該正当性確認処理によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加える変更処理と、（５）前記操作要求を行った指示者の電子署名を作成して、前記変更処理によって変更されたチームデータリストに該電子署名を添付して前記要求先に送付する処理とをコンピュータに実行させる。

【0075】

また、上述のチームデータリスト管理プログラムにおいて、前記正当性確認処理は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報を前記管理者情報として用いるものであっても良い。

また、上述のチームデータリスト管理プログラムは、前記ルートチームのチー

ムマスタの本人識別を行うための識別情報を所定の場所から取得して予め登録しておく処理と、前記要求先から前記ルートチームのオーソリティデータが送られてくる度に、予め登録されている前記識別情報を用いて、該オーソリティデータの電子署名が前記チームマスタの電子署名であることを確認する処理とをさらにコンピュータに実行させるものであっても良い。

【0076】

一方、チームを階層化するためのチームデータリストを保管するチームデータリスト保管プログラムを記録した記録媒体において、チームデータリスト保管プログラムは、（１）自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータをチーム毎に予め記憶しておく処理と、（２）自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストをチーム毎に予め記憶しておく処理と、（３）所定の要求元から前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する操作要求があったときに、該操作要求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、該操作要求が参照要求或いは削除要求である場合は、要求されたチームデータリストを前記要求元へ返送し或いは削除し、該操作要求が更新要求である場合は、前記要求元から送られるチームデータリストの電子署名が権限を持つ者による署名であることを前記管理者情報を用いて確認したのち、前記送られたチームデータリストで記憶されている前記オーソリティデータ及び記憶されている前記オーソリティリストを更新する権限確認処理とをコンピュータに実行させる。

また、上述のチームデータリスト保管プログラムにおいて、前記権限確認処理は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報を前記管理者情報として用いるものであって良い。

【0077】

【発明の効果】

以上説明したように、本発明では、オーソリティリストとオーソリティデータの含まれたチームデータリストを用いることで各チームの下にサブチームを作成することができ、階層化されたチームを構築することができる。また、ユーザはルートチームのチームマスタの署名を確認するだけで、操作対象のチームからルートチームに至る各チームについてチームデータリストの正当性を確認することができる。さらに、親チームの管理者の指示によって誰もがサブチーム内の管理を行うチームマスタになることができる。

また、本発明では、チームデータリストを親チームの管理下にあるオーソリティデータと自チームの管理に関わるオーソリティリストに分割しており、各チームのチームマスタが親チームの干渉を受けることなく情報共有メンバの管理といった自チーム内の管理を行うことができ、一方で、親チームの管理者はサブチーム内部の管理に関与する必要がなくなる。

また、本発明では、チームデータリストに対して正当な権限を持つ者による電子署名を含ませているため、改竄等の不正な行為を検出することが可能となる。

また、本発明では、チームデータリストの操作要求がなされた場合に、これら要求の指示者が権限を持つ者かどうかの権限確認を実施しているので、サーバの管理者、チーム内の一般のメンバ、クラッカ等の権限を持たない者による不正な行為を未然に防止することができる。

また、本発明では、特に選定されたチームマスタと一人以上のサブオーソリティに対してサブチームの管理権限を与えており、チームマスタ自身がサブオーソリティを選任できるほか、複数の管理者がサブチームを管理できるため管理負担が分散される。

また、本発明では、公開鍵などのルートチームのチームマスタ本人を識別・認証するための識別情報を予め登録しておき、この識別情報をもとに、ルートチームのチームマスタを確認しているため、チームデータリストを操作する度にユーザ自身が目視で確認するなどの煩わしい作業が必要なくなり、ルートチームのチームマスタを自動的に承認することが可能となる。

【図面の簡単な説明】

【図1】 本発明の第1実施形態によるチームデータリスト管理装置及びチ

ームデータリスト保管装置を有するシステムの構成を示したブロック図である。

【図 2】 同実施形態において、チームデータリスト保管装置が設置されたサーバ側に記憶されるチームデータリストの構造を示した説明図であって、(a) はオーソリティデータの構造、(b) はオーソリティリストの構造、(c) はオーソリティデータの簡略化表記、(d) はオーソリティリストの簡略化表記である。

【図 3】 同実施形態におけるチームの階層の一例を示した説明図である。

【図 4】 図 3 に示すチーム階層の各チームについてチームデータリストの具体的な値を記入した説明図である。

【図 5】 同実施形態においてサブチームを作成するための処理手順を示した説明図である。

【図 6】 図 5 の処理過程でサブチーム作成要求時に行われるサーバ側の権限確認機能についてその処理手順を示した説明図である。

【図 7】 図 5 の処理過程で実施されるクライアント側のリスト正当性検証に関わる処理手順を示した説明図である。

【図 8】 図 5 の処理過程において、クライアント側で新規に作成したチームデータリストをサーバ側で権限確認を行う際の処理手順を示す説明図である。

【図 9】 同実施形態において、サブチームのチームマスタを変更するための処理手順を示した説明図である。

【図 10】 同実施形態において、サブオーソリティの作成権限を変更（削除）するための処理手順を示した説明図である。

【図 11】 同実施形態において、サブチームを削除するための処理手順を示した説明図である。

【図 12】 クライアント側に居るユーザの権限確認を行う際にサーバが用いるシェイクハンドないしチャレンジレスポンスと呼ばれる手法の手順を示した説明図である。

【図 13】 本発明の第 2 実施形態におけるチームの階層の一例を示した説明図である。

【図 14】 本発明の第 3 実施形態におけるチームの階層の一例を示した説

明図である。

【図 15】 アクセス制御リストを利用して情報共有を行う従来のシステムの構成を示したブロック図である。

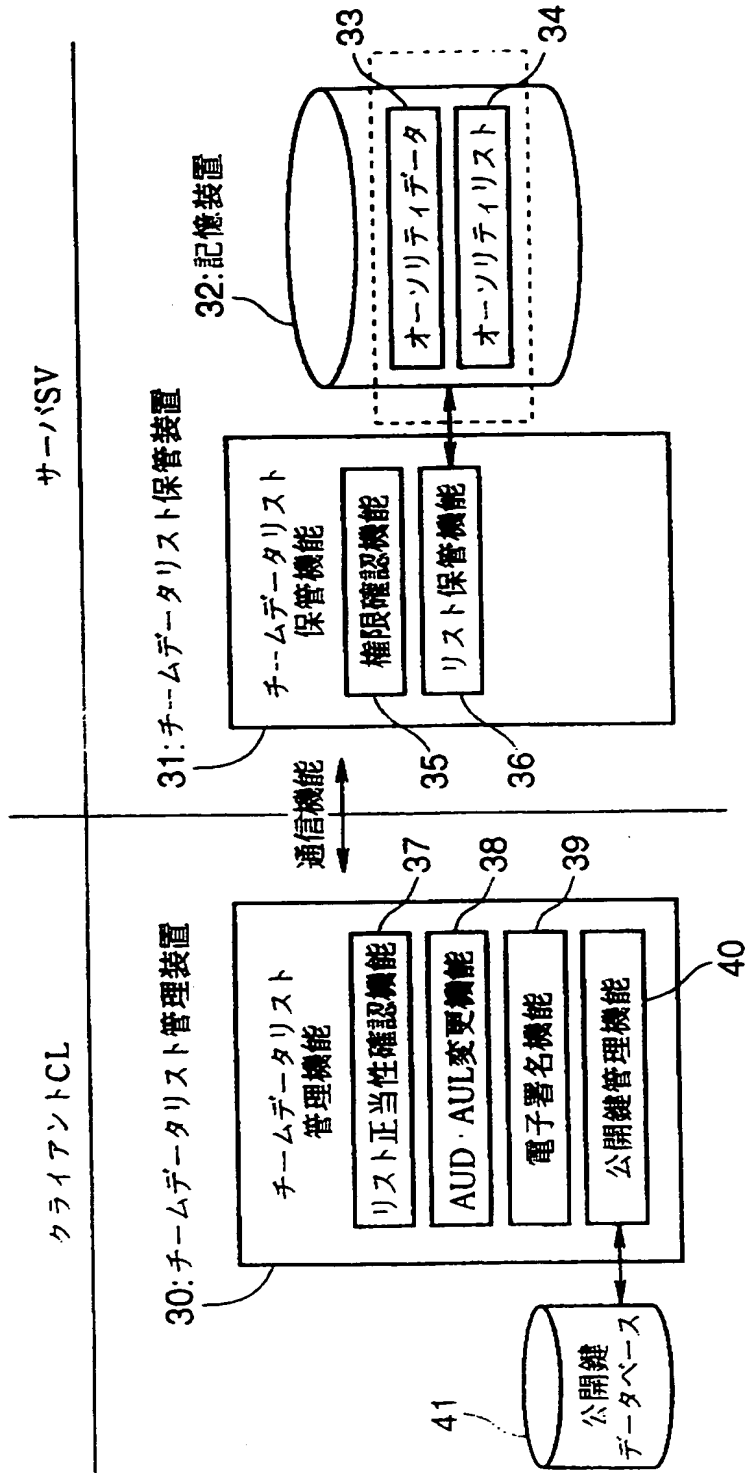
【符号の説明】

30…チームデータリスト管理装置、31…チームデータリスト保管装置、32…記憶装置、33…オーソリティデータ、34…オーソリティリスト、35…権限確認機能、36…リスト保管機能、37…リスト正当性確認機能、38…AUD・AUL変更機能、39…電子署名機能、40…公開鍵管理機能、41…公開鍵データベース、CL…クライアント、SV…サーバ

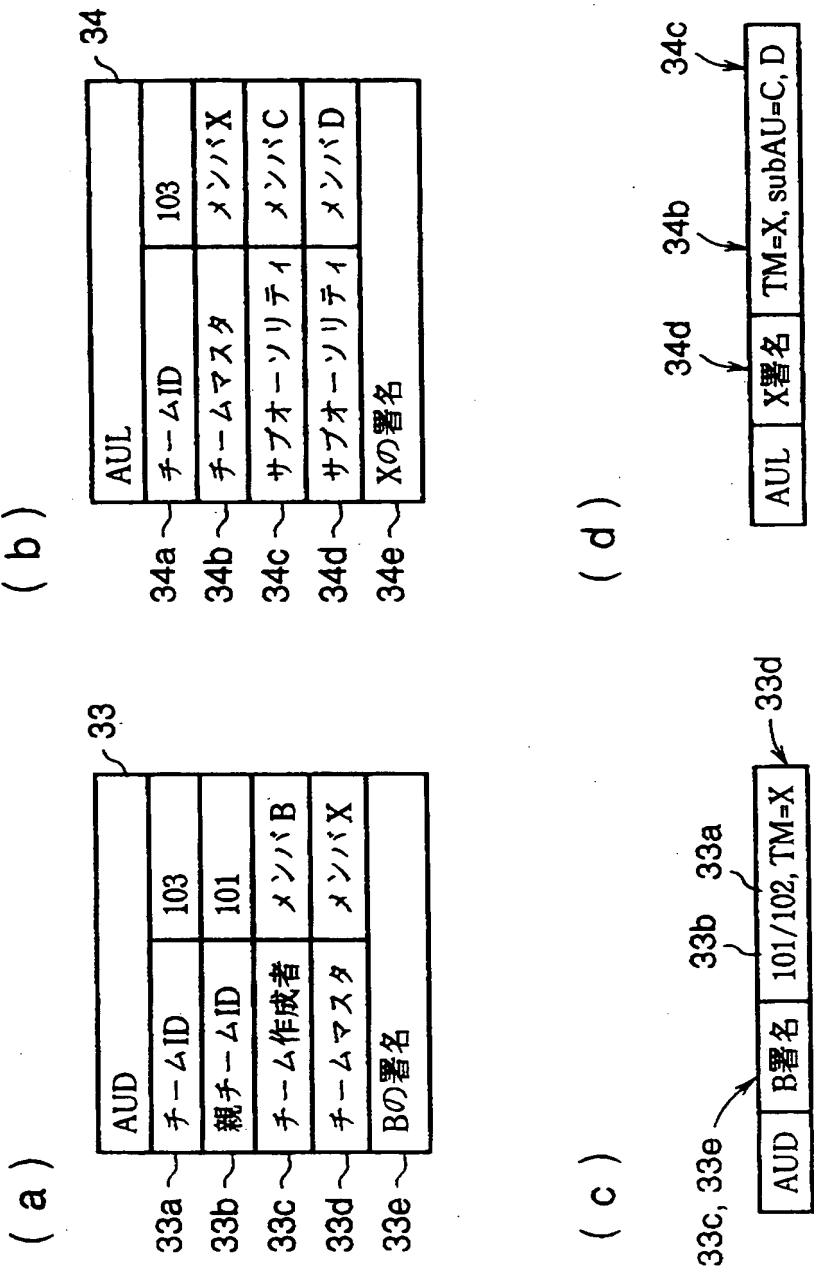
【書類名】

図面

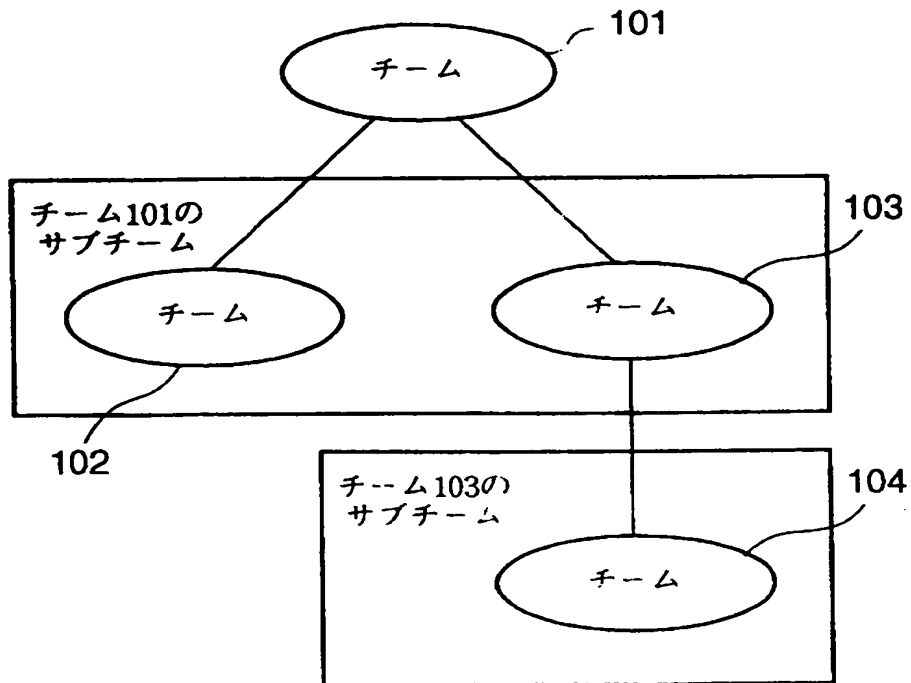
【図 1】



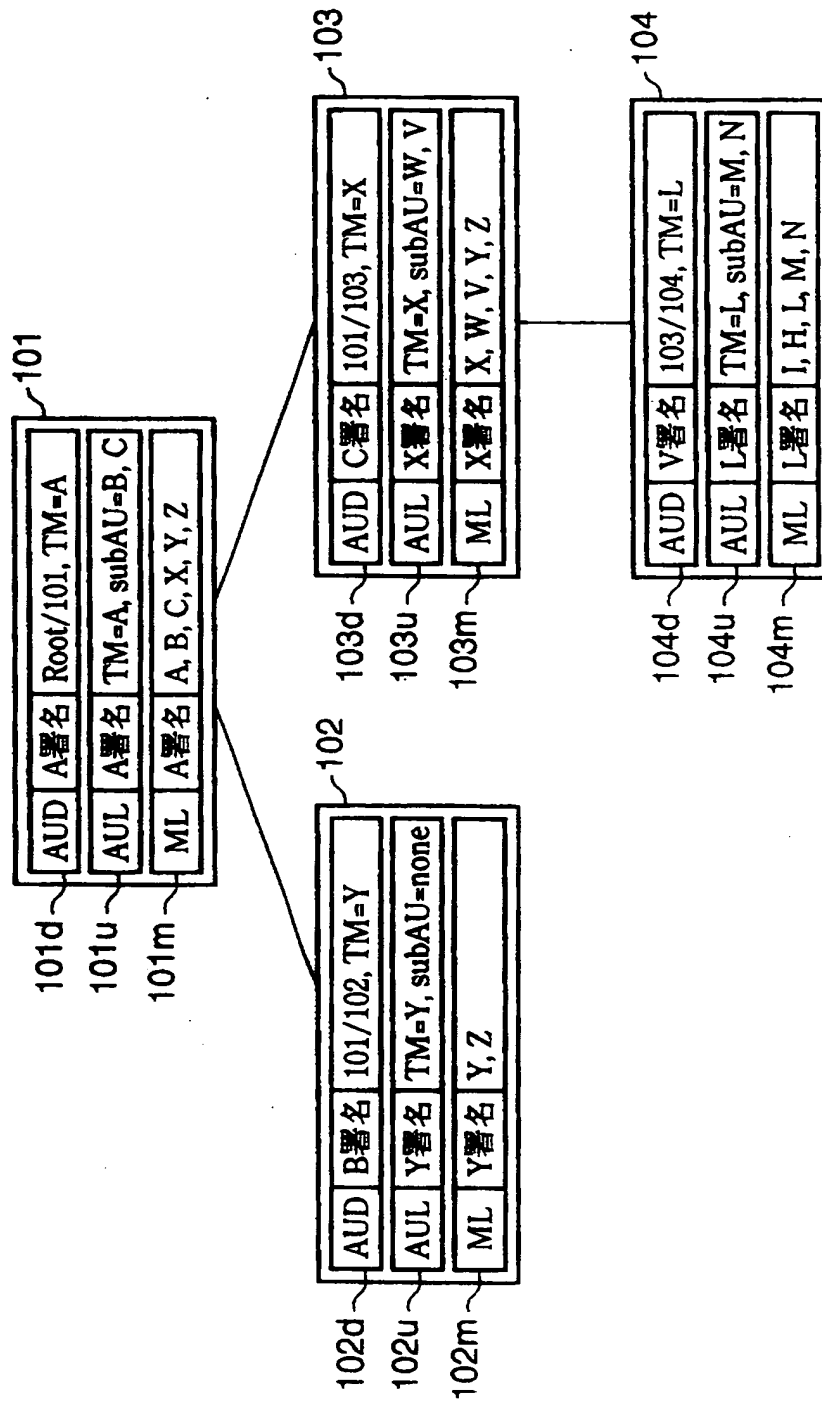
【図2】



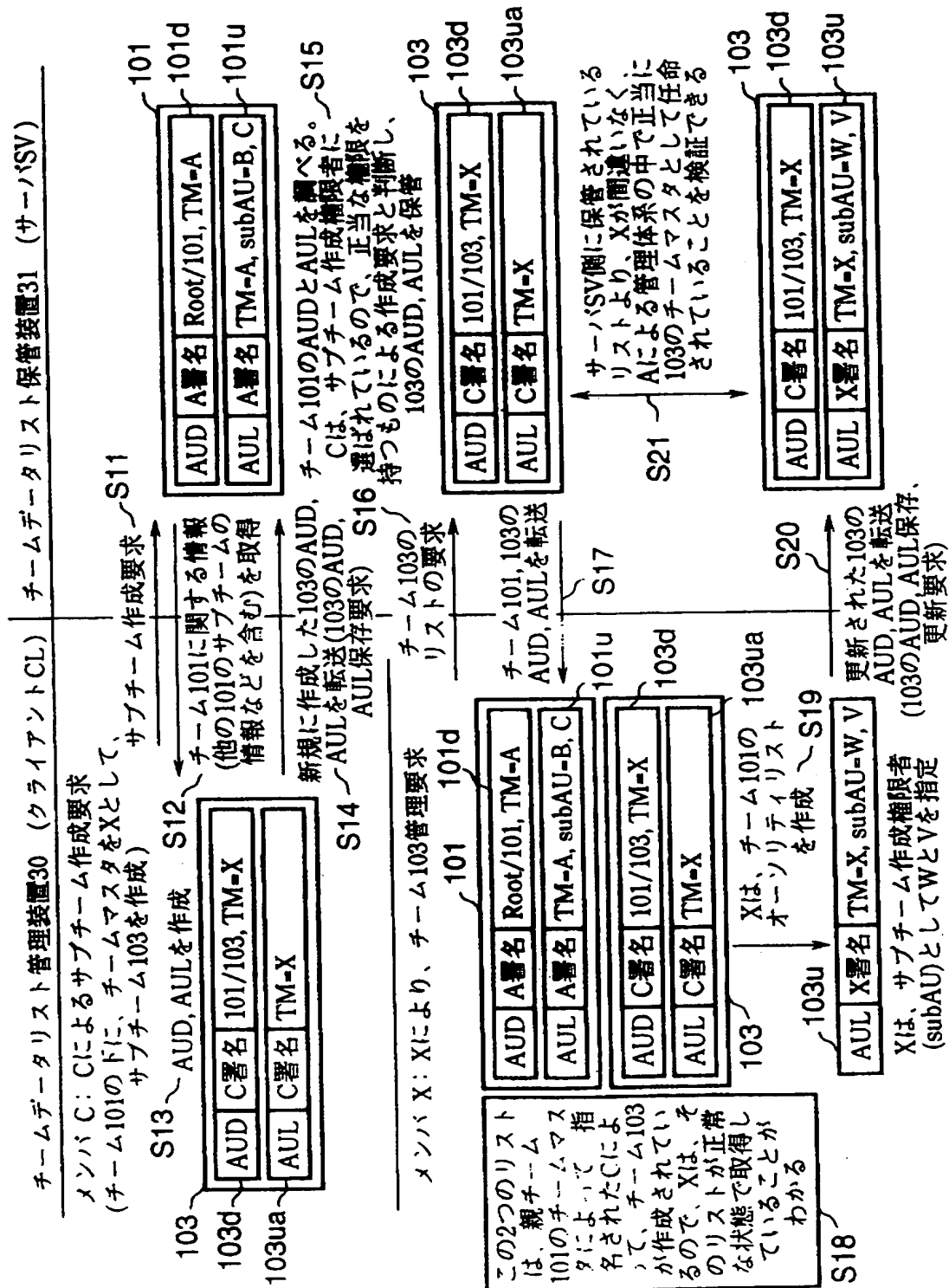
【図3】



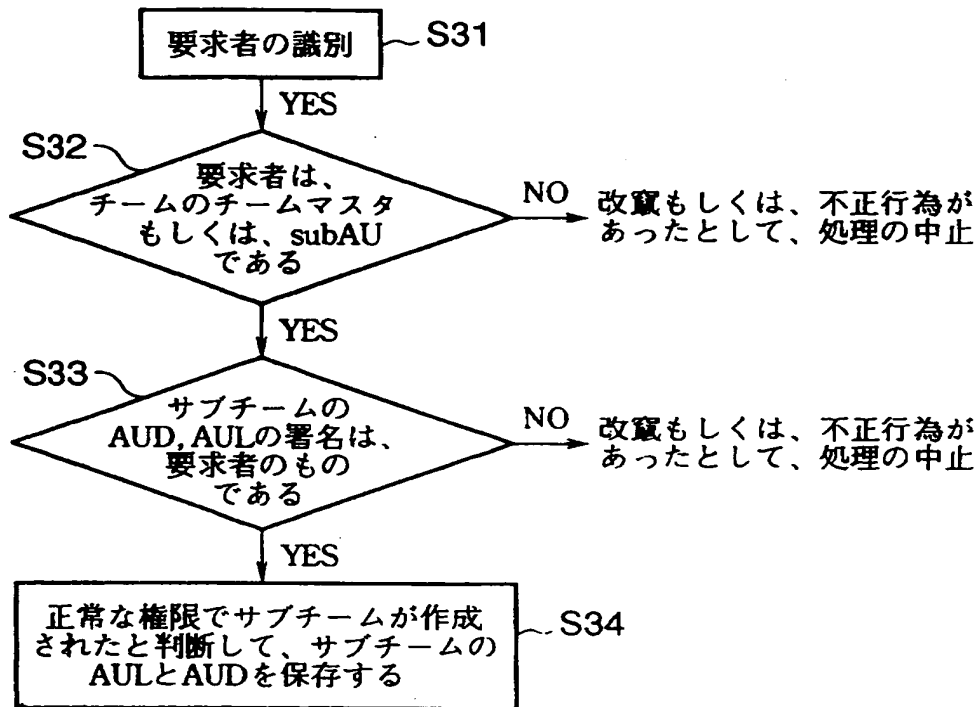
【図 4】



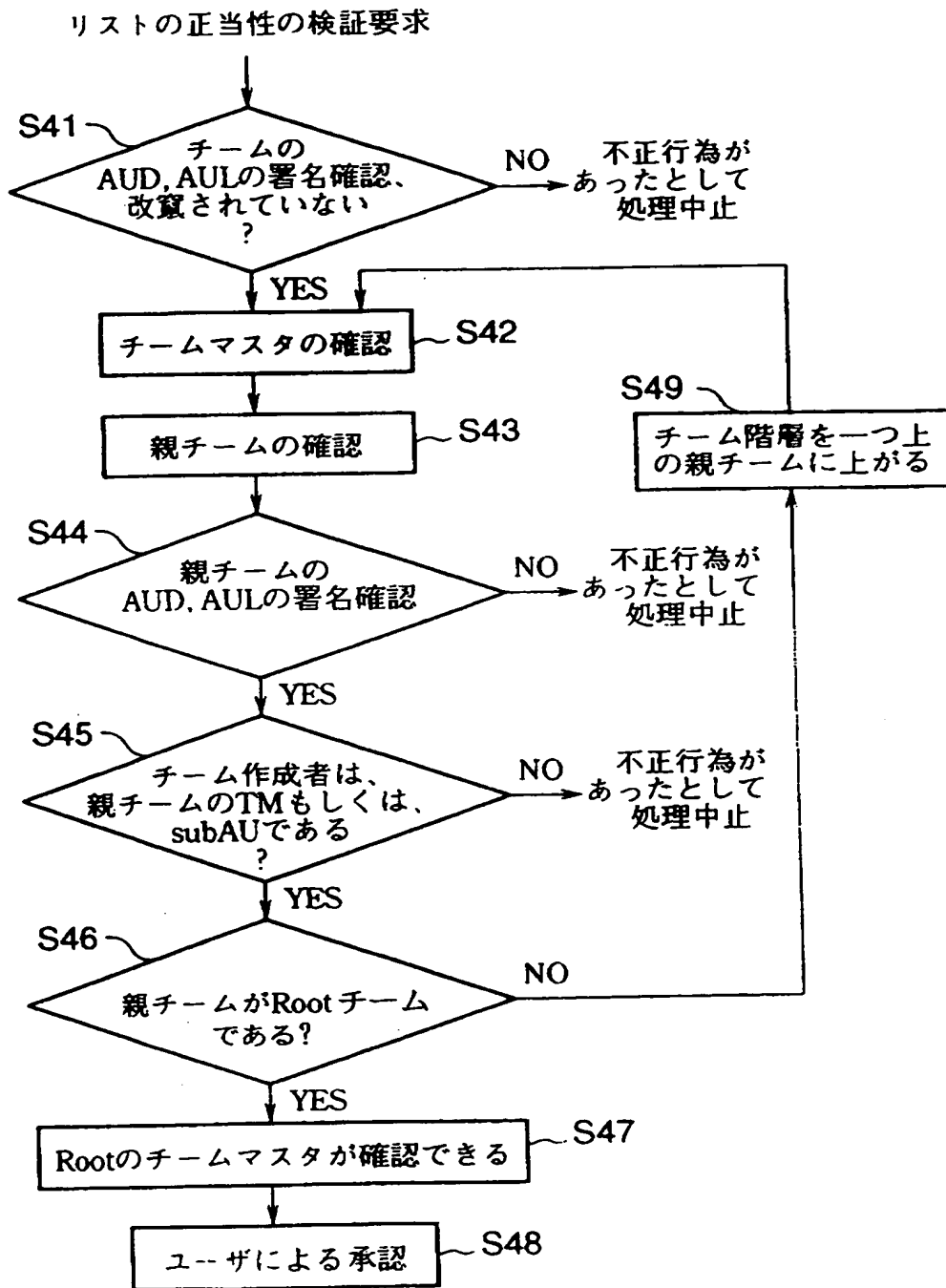
【図5】



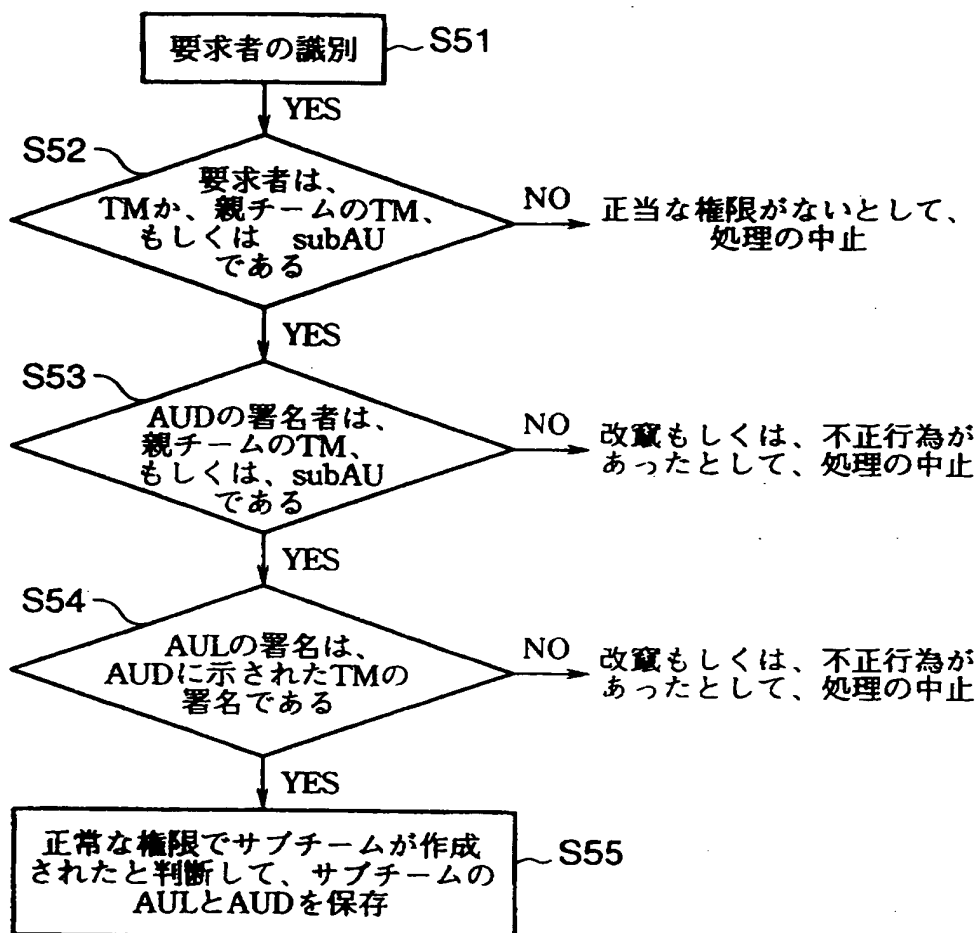
【図6】



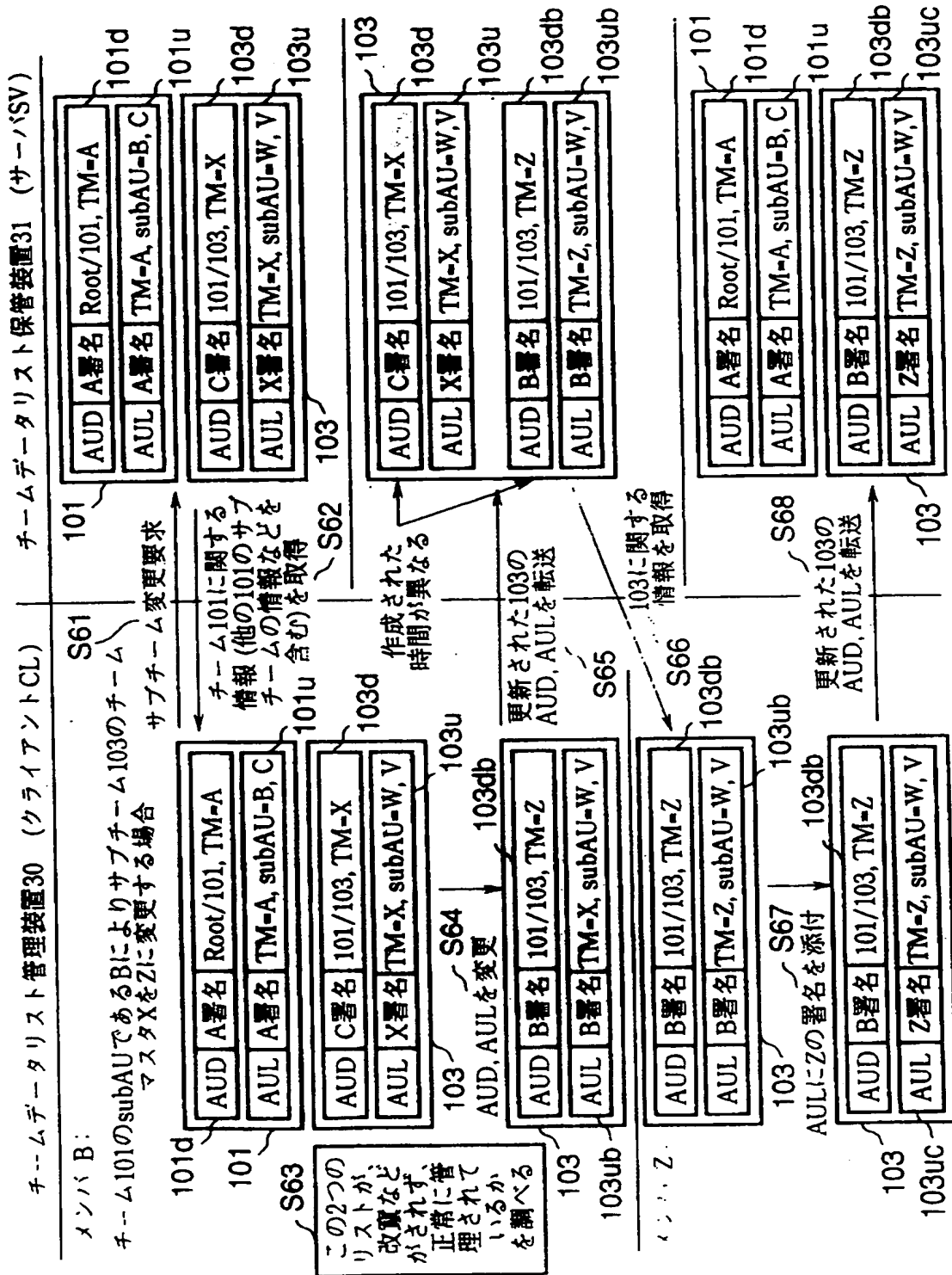
【図7】



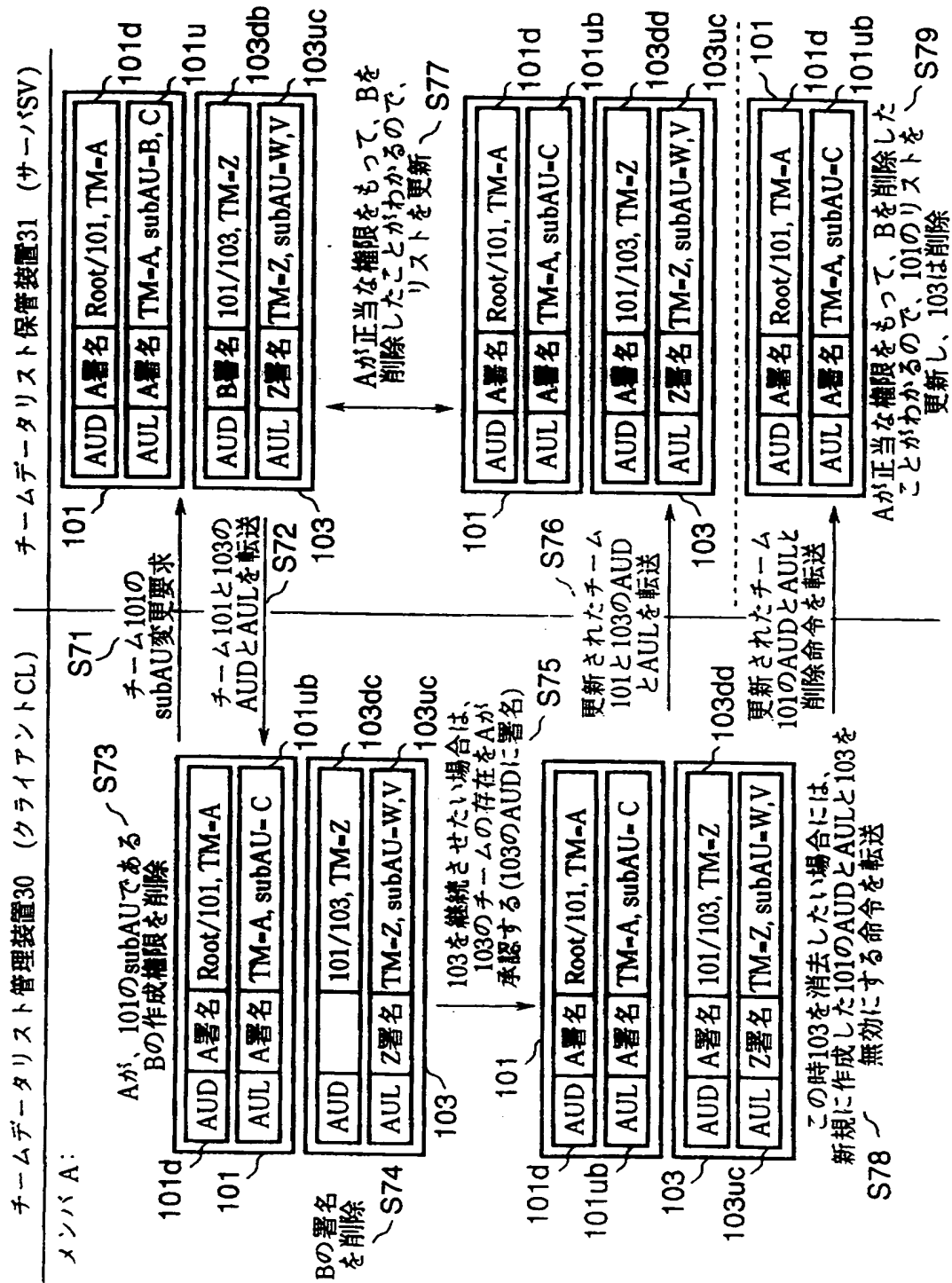
【図8】



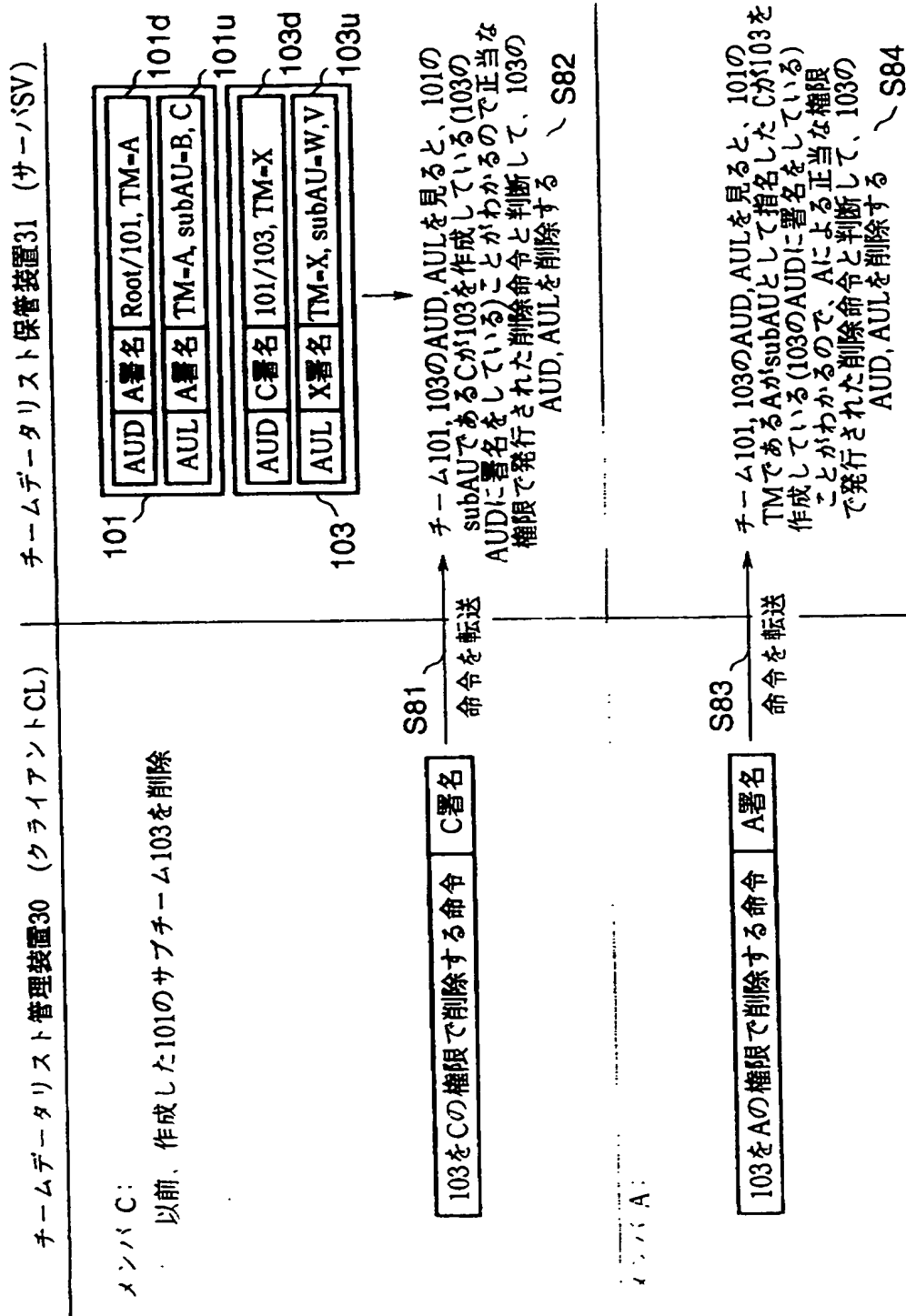
【図9】



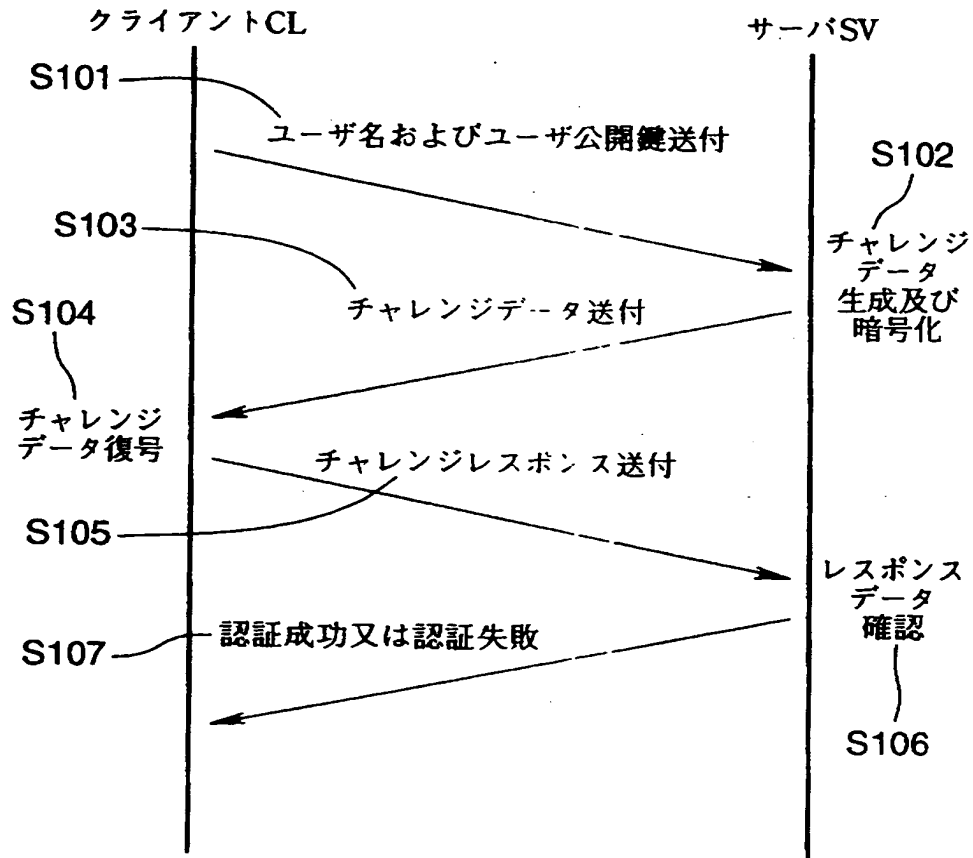
【図 1 0】



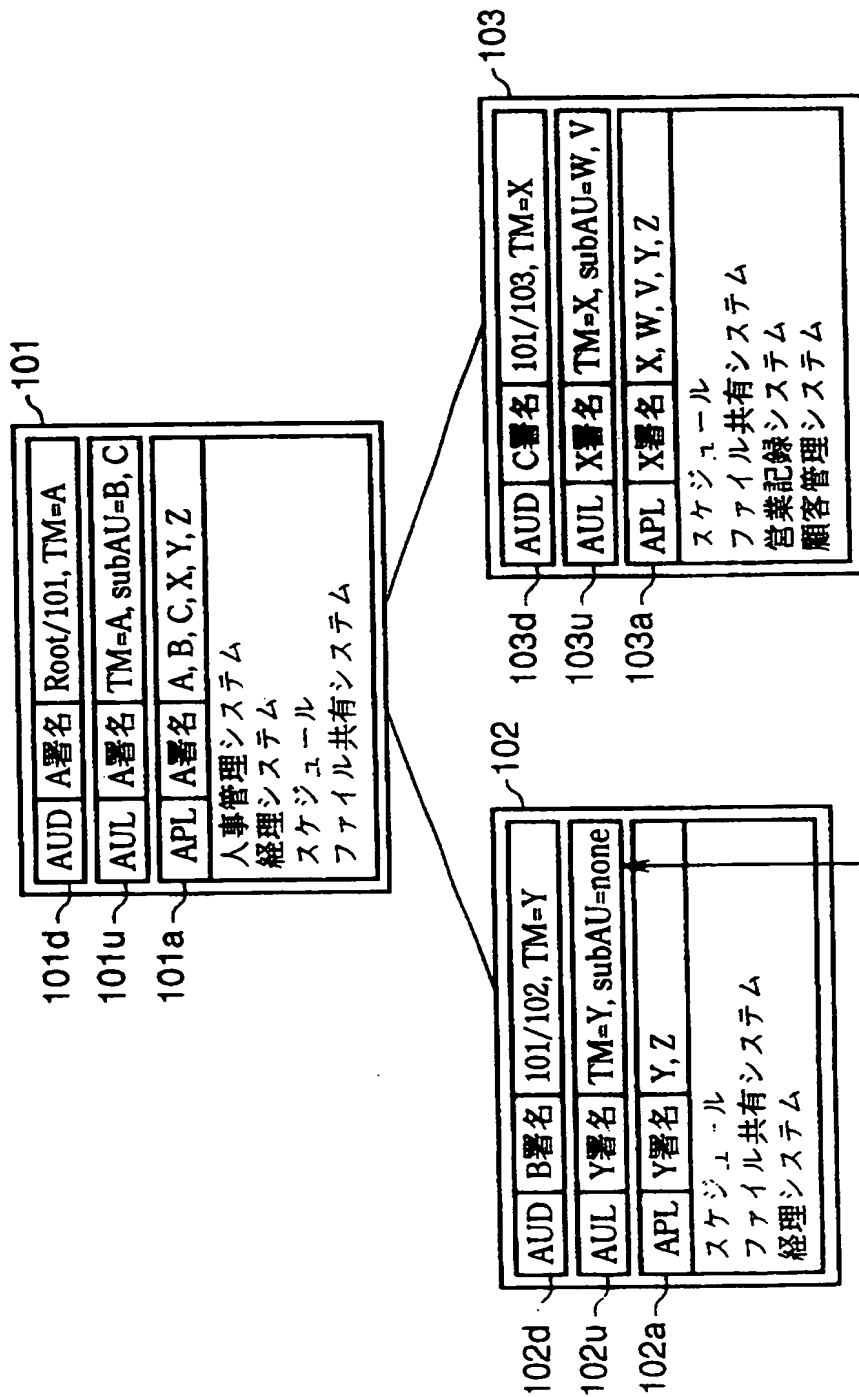
【図 11】



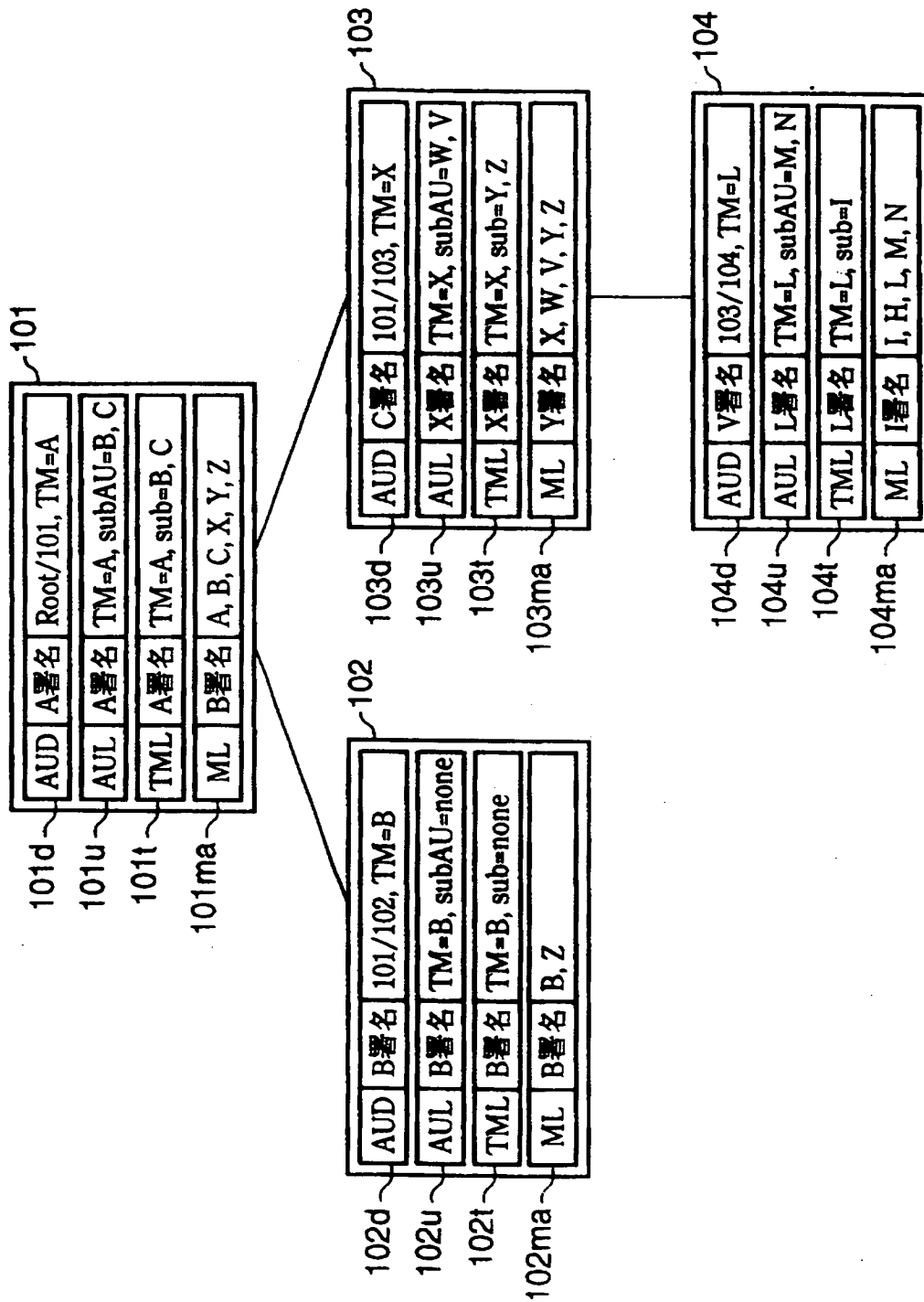
【図12】



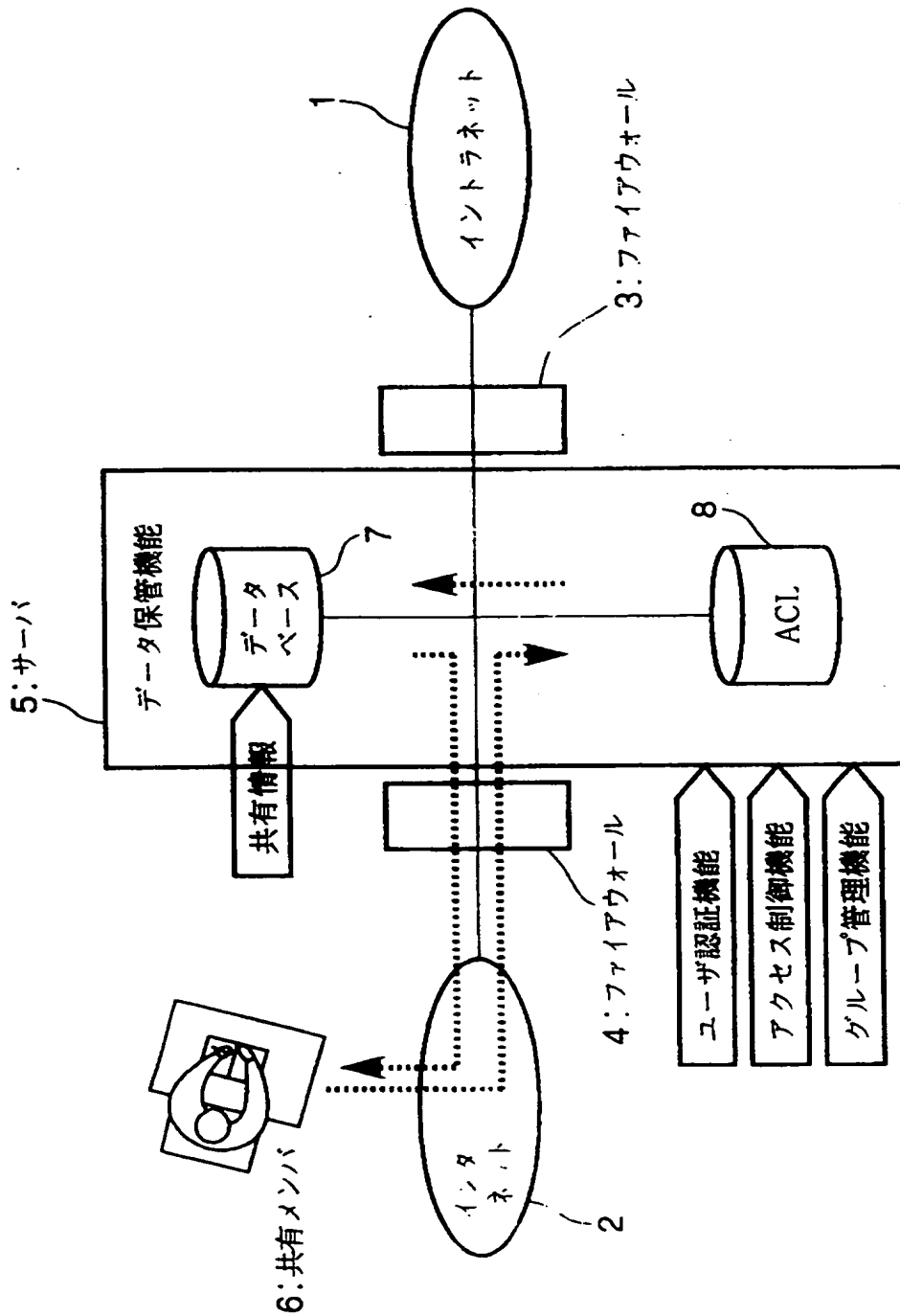
【図 13】



【图 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 複数のメンバで構成されるチームを階層化しつつ、情報や機能を共有できるチームデータリスト処理システムを提供する。

【解決手段】 オーソリティデータ33はチームとその配下のサブチームの関係を表すデータ、オーソリティリスト34は各チーム内の管理者を登録したリストであり、これらチームデータリストでチームの階層を規定する。リスト保管機能36は記憶装置32との間でチームデータリストを授受する。権限確認機能35はチームデータリストの参照、変更、削除要求時にチームデータリストの内容を基に要求の許可、拒否を判断する。リスト正当性確認機能37はチームデータリストの階層をルートチームに至るまで辿ってそのチームマスタの署名を確認する。AUD・AUL変更機能38はチームデータリストの作成、削除、変更を行う。電子署名機能39は公開鍵に対応する秘密鍵を取得し、変更されたチームデータリストに署名を付加する。

【選択図】 図1

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000006264
【住所又は居所】 東京都千代田区大手町1丁目5番1号
【氏名又は名称】 三菱マテリアル株式会社

【代理人】

申請人

【識別番号】 100064908
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル
志賀国際特許事務所

【氏名又は名称】 志賀 正武

【選任した代理人】

【識別番号】 100108578
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル
志賀国際特許事務所

【氏名又は名称】 高橋 詔男

【選任した代理人】

【識別番号】 100089037
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル
志賀国際特許事務所

【氏名又は名称】 渡邊 隆

【選任した代理人】

【識別番号】 100101465
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル
志賀国際特許事務所

【氏名又は名称】 青山 正和

【選任した代理人】

【識別番号】 100094400
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル
志賀国際特許事務所

【氏名又は名称】 鈴木 三義

【選任した代理人】

【識別番号】 100106493
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル
志賀国際特許事務所

【氏名又は名称】 松富 豊

【選任した代理人】

【識別番号】	100107836
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビル 志賀国際特許事務所
【氏名又は名称】	西 和哉
【選任した代理人】	
【識別番号】	100108394
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビル 志賀国際特許事務所
【氏名又は名称】	今村 健一
【選任した代理人】	
【識別番号】	100108453
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビル 志賀国際特許事務所
【氏名又は名称】	村山 靖彦
【選任した代理人】	
【識別番号】	100100077
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビル 志賀国際特許事務所
【氏名又は名称】	大場 充

出 願 人 履 歴 情 報

識別番号 [000006264]

1. 変更年月日	1992年 4月10日
[変更理由]	住所変更
住 所	東京都千代田区大手町1丁目5番1号
氏 名	三菱マテリアル株式会社

This Page Blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)